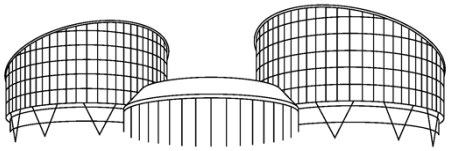

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

THIRD SECTION

CASE OF GREEN ALLIANCE v. BULGARIA

(Application no. 6580/22)

JUDGMENT

Art 8 • Home • Correspondence • Shortcomings in the legal framework permitting the infiltration of "agents on cover" into private organisations and "liberal professions" • Application by analogy of case-law principles developed in relation to covert surveillance • Work of an "agent on cover" could interfere with the applicant association's rights • Mere existence of the relevant regulations amounting to an interference with the applicant association's rights • Examination of the legal framework in the abstract • Lack of minimum safeguards against arbitrariness and abuse • Quality-of-law requirement not met

Prepared by the Registry. Does not bind the Court.

STRASBOURG

17 February 2026

This judgment will become final in the circumstances set out in Article 44 § 2 of the Convention. It may be subject to editorial revision.

TABLE OF CONTENTS

In the case of Green Alliance v. Bulgaria,

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

Ioannis Ktistakis, *President*,
Peeter Roosma,
Darian Pavli,
Úna Ní Raifeartaigh,
Mateja Đurović,
Vasilka Sancin, *judges*,
Mira Raycheva, ad hoc *judge*,
and Milan Blaško, *Section Registrar*,

Having regard to:

the application (no. 6580/22) against the Republic of Bulgaria lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by an association with a registered office in Bulgaria, Green Alliance ("the applicant association" or "the association"), on 19 January 2022;

the decision to give the Bulgarian Government ("the Government") notice of the application;

the parties' observations;

the decision of the President of the Section to exempt Diana Kovatcheva, the judge elected in respect of Bulgaria, from sitting in this case and his ensuing decision to appoint Mira Raycheva to sit as *ad hoc* judge in the case;

Having deliberated in private on 27 January 2026,

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

INTRODUCTION

1. Under regulations issued in 2008 and amended in 2018, Bulgaria's State Agency for National Security ("the Agency") can, on the decision of its head, infiltrate "agents on cover" (*служители на прикритие*) into a private entity or as members of a "liberal profession". Those "agents on cover" conceal only that they are working for the Agency, but are not permitted to use covert surveillance techniques or equipment, and are in Bulgaria considered as different from "agents under cover". The applicant association sought judicial review of those regulations, arguing that in the absence of effective safeguards in relation to the use of such agents, they permitted abusive and disproportionate interferences with rights protected under Article 8 of the Convention. The administrative courts dismissed its claim.

2. The main issues in the case are (a) whether the association can claim to be a victim of interference with its rights under Article 8 of the Convention by reason of the mere existence of the regulations permitting the deployment of "agents on cover", and (b) if so, whether that inference is compatible with that Article.

THE FACTS

3. The applicant association was founded in 2006 and has its registered office in the town of Kostenets, in the Sofia Region. It was represented by Mr T. Trifonov, a lawyer practising in Sofia.

4. The Government were represented by their Agent, Ms B. Simeonova of the Ministry of Justice.

I. THE APPLICANT ASSOCIATION

5. The association's objectives, as set out in its articles of association, concern issues relating to the protection of the environment.

II. THE REGULATIONS ON "AGENTS ON COVER"

A. As originally issued in 2008

6. Acting pursuant to a general statutory delegation in paragraph 43 of the transitional and concluding provisions of the State Agency for National Security Act 2007 ("the 2007 Act"), which governs the work of the Agency, in February 2008 the Government issued Regulations governing the application of that Act. They were published in the Bulgarian State Gazette later that month (*ДВ, бр. 17 от 19.02.2008 г., стр. 7-17*), and took effect following the expiry of three days after the date of their publication (in line with the general rule set out by Article 5 § 5 of the Bulgarian Constitution and section 41(3) and (4) of the Normative Instruments Act 1973).

7. Part 1 of Chapter 5 of those Regulations, comprising regulations 49-62, laid down the regime for the so-called "agents on cover" (*служители на прикритие*), which the Regulations distinguished from "agents under cover" (*служители под прикритие*), which are regulated elsewhere in Bulgarian law (see paragraphs 74 (h) and 75 below).[1]

8. By regulation 49, the use of "agents on cover" and their work must comply with the principles of lawfulness and clandestineness.

9. As initially worded, regulation 50 permitted the Agency to infiltrate "agents on cover" into State authorities, organisations and legal persons.

10. Regulation 51 specifies that (a) "agents on cover" are officers of the Agency who have a special status and the rights and duties pertaining to the position in which they are infiltrated, and that (b) only civil servants who have already undergone initial training and have obtained security clearance

[1] In 2013-15, when the Agency had – on top of its main task of safeguarding national security – also the task of investigating criminal offences relating to national security (see paragraph 42 *in fine* below), it could deploy "agents under cover" as well. Their use was governed by regulations 62a-62l, added in December 2013 and repealed in June 2015.

permitting them to access classified information may become "agents on cover".

11. "Work on cover" by such agents is possible if there is a "proven operational need" (regulation 52(1)). Such a need exists if the Agency's statutory tasks cannot be discharged in another way (regulation 52(2)). The head of the respective division or unit of the Agency must prove the existence of such an operational need to the Agency's head (regulation 52(3)).

12. "Agents on cover" may carry out intelligence and counterintelligence work for the protection of national security (regulation 53(1)). Their precise tasks are to be set by the head of the Agency in each individual case (regulation 53(2)). They may not arrest, search, or interrogate people, or use firearms or physical force (regulation 53(3), read in conjunction with the relevant sections of the 2007 Act).

13. They must work in a way that does not risk exposing their cover (regulation 54).

14. As originally worded (before 2018 amendments to the Regulations – see paragraphs 18-30 below), regulation 55(1) envisaged that Agency officers would be appointed as "agents on cover" by the head of the target entity upon a request by the head of the Agency. An existing employee of the target entity could also be appointed as an "agent on cover" by means of being engaged as an Agency officer (regulation 55(2)).

15. The appointment procedure before the 2018 amendments was as follows. The head of the Agency was to make a request to the target entity, identify the positions in that target entity that could be suitable for the infiltration of an "agent on cover", and designate a contact officer from the Agency (regulation 56 (1)). If the target entity agreed, it was to inform the Agency about the skills and qualifications that the "agent on cover" had to have, and about the procedure to be followed when appointing someone to the target position (regulation 56(2)). The target entity could also suggest amendments to the rules or regulations governing its work in order to accommodate the possibility to infiltrate an "agent on cover" (regulation 56(3)). The head of the Agency and the target entity were then to coordinate how exactly the "agent on cover" would be infiltrated (regulation 56(4). The target entity had to treat all those organisational matters as classified information (regulation 56(5)).

16. The target entity was then under a duty to assist the "agent on cover" in the performance of his or her duties (regulation 56(6)). It had to be advised by the Agency if the "work on cover" was to be stopped (regulation 57(2)). The target entity had to take the necessary measures not to permit "work on cover" to be revealed, even after its end (regulation 58(1)).

17. Regulations 59-62 govern the employment rights of "agents on cover" in respect of pay, annual leave, and retirement.

B. The 2018 amendments

1. Proposal by the Agency for those amendments

18. In April 2018 the Agency proposed to the Government that regulations 50, 51 and 55 be reworded and that regulations 56-58 be repealed (see paragraphs 9-10 and 14-16 above). In its view, those amendments – whose effect would be to expand the list of potential target entities and do away with the requirement to obtain the target entity's assent to infiltration – were needed because practice showed that the way in which the regulations structured the infiltration of "agents on cover" prevented their quick and efficient use in a dynamically changing security environment that required timely and adequate responses to encroachments on national security. The existing procedure did not meet the Agency's need to obtain the accurate information necessary for that purpose. In particular, the requirement to obtain the target entity's assent posed a problem with respect to entities whose heads were unwilling to cooperate. Moreover, the categories of entities in which "agents on cover" could be infiltrated were too limited and did not reflect modern economic realities.

2. Public consultation about that proposal

19. During the ensuing public consultation, opened in May 2018 and concluded in June 2018, comments were received from an association, the Bulgarian Helsinki Committee, and from the Supreme Bar Council (the governing body of Bulgaria's National Bar).

(a) Comments by the Bulgarian Helsinki Committee

20. The Bulgarian Helsinki Committee opposed the proposed amendments as a whole. It pointed out that, as attested by the Agency's practice in relation to the expulsion of aliens, no specific facts were normally cited in support of its assertions that someone was a national security risk, and that this phrase was employed declaratively – anything could be made to fit the term. It could therefore be presumed that the same approach would be taken to the infiltration of "agents on cover", which under the proposed amendments could be undertaken in respect of any private organisation or members of any "liberal profession" – accountants, auditors, journalists, lawyers – which would affect the clients of any such professionals. That was especially dangerous in the light of the Agency's well-documented stance that it was above the country's laws and in the light of the secrecy of its work. There were therefore no guarantees that the right to respect for private life would not be unlawfully interfered with. In particular, no judicial supervision was envisaged in relation to the use of "agents on cover", nor any time-limits in respect of such use. Some sort of supervisory mechanism similar to that provided by law in respect of "special means of surveillance" (for the

definition of that term in Bulgarian law, see *Ekimdzhiev and Others v. Bulgaria*, no. 70078/12, § 11, 11 January 2022; see also paragraphs 73-74 below) was indispensable.

(b) Comments by the Supreme Bar Council

21. The Supreme Bar Council took issue in particular with the possibility under the proposed amendments for "agents on cover" to be infiltrated as lawyers in private practice. In its view, that would contravene basic tenets of the Convention, the Constitution, the Bar Act 2004 and the Bar Code of Ethics, since it would enable "agents on cover" to pose as lawyers and – instead of providing legal advice and assistance – harm the people who consulted them as clients. Even the mere suspicion by clients that their lawyers could be "agents on cover" could ruin public confidence in the legal profession. Moreover, the infiltration of Agency officers as lawyers, or in any "liberal profession", went beyond its statutory mandate. The Agency could fulfil its functions even in the absence of such a possibility. It had not explained specifically why it needed it. Nor had it pointed to the legitimate aim which that possibility would pursue – and that possibility seemed anyhow disproportionate to any such aim. It was therefore necessary to put language in the amendments that would make it plain that "agents on cover" could not be infiltrated as lawyers in private practice.

(c) Response by the Agency

22. In response, and having met in August 2018 with representatives of the Bulgarian Helsinki Committee and the Supreme Bar Council to hear their misgivings about the proposed amendments and explain the need for them, in early September 2018 the Agency wrote to the Minister of Internal Affairs.

23. The Agency stated, in relation to the concerns expressed by the Bulgarian Helsinki Committee (see paragraph 20 above), that those stemmed from a misunderstanding about the meaning that the competent authorities ascribed to the term "national security" and, more generally, about how those authorities operated. It was normal for their work to be secret. For its part, the term "national security" had been defined by statute (see paragraph 77 below), and it could not be said that it was being employed in a blanket manner in proceedings for the expulsion of aliens. In any event, no proper analogy could be drawn between that situation and the infiltration of "agents on cover". There was no reason to suppose that such infiltration would be undertaken unlawfully; under the 2007 Act the Agency had to act lawfully and within the scope of its statutory tasks in all circumstances, including when engaging in clandestine work. Nor was it apparent how such infiltration could infringe anyone's rights, especially since "agents on cover" remained fully liable for their acts.

24. It was also important to emphasise that "agents on cover" differed from "agents under cover". The latter constituted a kind of "special means of surveillance" governed by the Special Surveillance Means Act 1997 ("the 1997 Act" – see paragraphs 73-75 below). They operated under a false identity, could use technical devices to document evidence of offending, and bore no criminal liability for acts carried out in the course of their duties. The Agency was not among the authorities which could deploy "agents under cover". By contrast, "agents on cover" did not constitute a "special means of surveillance". They could not use technical devices to record evidence, and could bear criminal liability for their acts. It was true that they could gather information about encroachments on national security or about persons intending to engage in such acts. But that was not unlawful or something which could affect Convention rights. In fact, all members of the public were under a legal duty to bring to the attention of the authorities information about criminal conduct that came their way. The same went for any Agency officer who came to learn of an offence directed against national security. The work of "agents on cover" could not therefore be seen as a form of covert surveillance requiring judicial supervision. In any event, supervision could be carried out by Parliament and the Government, in a general way, as well as by the judiciary, in cases of unlawful conduct relating to the use of "agents on cover".

25. The Agency went on to state that the reservations of the Supreme Bar Council (see paragraph 21 above) were partly well-founded. Although the possibility for the Agency to infiltrate "agents on cover" into "liberal professions" in general did not exceed its statutory mandate, the position was different with regard specifically to the legal profession. Even when the proposed amendments had been drafted initially, the understanding had been that "agents on cover" could not be infiltrated as lawyers in private practice. It was in any case preferable to avoid speculation on that point. The Supreme Bar Council's suggestion that the proposed amendments be modified so as to clarify that "agents on cover" could not be infiltrated as lawyers in private practice therefore had to be accepted. The draft amendments had been revised accordingly.

(d) Adoption of the amendments

26. In September 2018 the Government adopted the amendments, as revised by the Agency in response to the Supreme Bar Council's comments. They were published in the Bulgarian State Gazette later that month (see *Постановление № 206 на Министерския съвет от 20.09.2018 г. за изменение и допълнение на Правилника за прилагане на Закона за Държавна агенция „Национална сигурност“, обн., ДВ, бр. 79 от 25.09.2018 г., стр. 3-4*), and took effect following the expiry of three days following the date of their publication (in line with the general rule set

out by Article 5 § 5 of the Bulgarian Constitution and by section 41(3) and (4) of the Normative Instruments Act 1973).

3. Text of the amendments

27. The amendments reworded regulations 50, 51 and 55, and repealed regulations 56-58 (see paragraphs 9-10 and 14-16 above).

28. Under the new wording of regulation 50 (see paragraph 9 above), "agents on cover" may be infiltrated into the State administration, into legal persons and into civil associations, and as persons exercising a "liberal profession" (except as lawyers in private practice).

29. The wording of regulation 51 (see paragraph 10 above) was amended in such a manner as to clarify that the position in which an "agent on cover" could be infiltrated was not limited to a position in a public entity.

30. Regulation 55 (see paragraph 14 above) was amended to state merely that Agency officers had to be infiltrated as "agents on cover" in a manner that did not risk the exposure of their cover.

III. JUDICIAL REVIEW OF THE AMENDED REGULATIONS

A. At first instance

1. Course of the proceedings

31. In October 2018 the applicant association sought judicial review of regulations 49-62, as partly amended in September 2018 (see paragraphs 6-30 above). It pointed out that the traditional term used in the legislation (specifically, the 1997 Act) to designate covert operatives was "agents under cover" (see paragraph 74 (h) and 75 below), whereas the term "agents on cover" could be found at the statutory level in only two provisions of the 2007 Act – sections 35a and 110(1)(7)(e) (see paragraph 48 below) – without, however, being defined or elaborated on in those provisions. There had therefore been no proper statutory delegation for the Government to issue regulations specifically relating to "agents on cover". The work of such agents could undoubtedly affect rights guaranteed by Article 8 of the Convention, since they could access covertly the in-house information or communications of any organisation, or could spy on its staff. The absence of statutory rules governing that work, and the resulting lack of safeguards against the misuse of "agents on cover", meant that their use would not be "in accordance with the law". The only means of ensuing compliance with that provision – in particular by appropriately limiting the length of time that such interference with rights could be carried out– was to subject the deployment of "agents on cover" to judicial supervision. Moreover, before issuing the Regulations the Government had not properly explained their purpose and

expected impact – particularly in respect of rights protected by Article 8 of the Convention, as construed by this Court.

32. The Agency, which intervened in the proceedings as an interested party, contested the claim. It argued, firstly, that the claim was inadmissible, because (a) the regulations did not touch on a matter falling within the aims of the applicant association, as set out in its articles, (b) the regulations permitted – but did not require – the infiltration of "agents on cover" into all legal persons, and (c) unlike "agents under cover" under the 1997 Act (see paragraph 74 (h) and 75 below), "agents on cover" were not permitted to carry out visual or aural surveillance. In the alternative, the claim was without merit because the purpose of the amended regulations had been explained during the public consultation preceding the adoption of the amendments. The claim confused "agents under cover" and "agents on cover". The regulations pursued a proper statutory purpose and fell within the statutory delegation given by the 2007 Act – which, in section 123(2)(6) (see paragraph 49 below), gave the Agency the power to conceal its officers and their work in a manner laid down in regulations for the application of the Act. No issue arose under Article 8 of the Convention, since the work of "agents on cover" did not entail unlawful intrusion into private life, home or correspondence. Their work was, in any event, not without external supervision – it could be supervised by Parliament and the government, pursuant to reports by members of the public to the Agency itself, and via the possibility to seek judicial review of any decisions of the Agency.

33. The government, which was the respondent to the claim, likewise argued that it was inadmissible – and in the alternative ill-founded – on the basis of arguments to the same effect as those made by the Agency.

34. In September 2019 the three-judge panel of the Supreme Administrative Court to which the claim had been assigned held that, in the light of its stated aims (as set out in its articles of association), the association had no standing to challenge the regulations. Non-governmental organisations could challenge statutory instruments only if those instruments directly and automatically affected their objects. That was not the case with the regulations in issue, which permitted (but did not automatically lead to) the deployment of "agents on cover" in non-governmental organisations (see *опр. № 12167 от 10.09.2019 г. по адм. д. № 13588/2018 г., ВАС, II о.*).

35. Following an appeal by the association, in December 2019 a five-judge panel of the Supreme Administrative Court quashed that decision and remitted the case to the three-judge panel for an examination on the merits. It held that in so far as they permitted the use of "agents on cover" in non-governmental organisations, the regulations directly affected the association's legal sphere. Its specific goals were irrelevant in that respect (see *опр. № 16975 от 11.12.2019 г. по адм. д. № 12578/2019 г., ВАС, петчл. с-в*).

2. Judgment of the Supreme Administrative Court

36. The three-judge panel then examined the claim on the merits. The applicant association, the Agency and the Government all referred to their earlier submissions regarding the merits of the case (see paragraphs 31-33 above).

37. In December 2020 the three-judge panel dismissed the claim. It noted that the 2007 Act had empowered the government to issue regulations in respect of its application, which in the panel's view meant that there had been proper statutory delegation for the impugned regulations. The procedure for issuing the regulations had been followed, and they contravened no higher-ranking rules. In particular, regulations 49-62 fully accorded with section 123(2)(6) of the 2007 Act, which authorised the Agency to place its officers under cover and organise their clandestine work in a manner set out in the regulations (namely, regulations 49-62) regarding the application of the Act (see paragraph 49 below). Section 110(1)(7)(e) likewise referred to "agents on cover" (see paragraph 48 (b) below). None of those provisions were inconsistent with any other of those provisions (see *реш. № 15819 от 21.12.2020 г. по адм. д. № 13588/2018 г., ВАС, II о.*).

B. On appeal

1. Course of the proceedings

38. The applicant association appealed on points of law. It submitted that the three-judge panel had not duly addressed its argument that the regulations had been made without proper statutory delegation, since the 2007 Act itself had neither defined "agents on cover" nor set out their role. Moreover, under Article 8 of the Convention and this Court's case-law, intrusions of the sort resulting from the use of "agents on cover" had to be surrounded by effective safeguards. The 1997 Act laid down many such safeguards – notably judicial supervision – with respect to "specials means of surveillance". Since "agents on cover" could likewise interfere with "private life" and "correspondence" – in particular that of the people working in the entities into which such agents would be infiltrated – such safeguards were required with respect to them as well; they were not inconsistent with the clandestine nature of those agents' work. There was no good reason to distinguish in that respect between "agents under cover" under the 1997 Act and "agents on cover" under the Regulations.

39. The Agency and the Government contested the appeal, referring to the same arguments that they had made before the three-judge panel (see paragraphs 32-33 above).

2. Judgment of the Supreme Administrative Court

40. On 19 July 2021 a five-judge panel of the Supreme Administrative Court upheld the three-judge panel's judgment. It agreed that there had been proper statutory delegation for the impugned regulations. It went on to state that the law distinguished between "agents under cover" and "agents on cover". An analysis of the statutory provisions governing the use of "special means of surveillance" indicated that unlike "agents under cover", "agents on cover" could not employ such means. It followed that the argument, based on the 1997 Act (see paragraphs 73-75 below), that any deployment of "agents on cover" had to be subject to prior judicial authorisation (as required by the 1997 Act with respect to "special means of surveillance") was without merit. Moreover, in view of the wording of regulation 50 (see paragraph 28 above), the work of an "agent on cover" could not affect someone's private life, home or correspondence. The assertion that the regulations contravened Article 8 of the Convention was therefore also baseless (see *реш. № 8672 от 19.07.2021 г. по адм. д. № 2863/2021 г., ВАС, петчл. с-в*).

RELEVANT LEGAL FRAMEWORK

I. 2007 ACT

A. The Agency, its tasks and powers

41. The 2007 Act – which created the Agency and defined its tasks and powers – was enacted in December 2007 and came into force in January 2008. By paragraph 2(2) and (3) of the Act's transitional provisions, the Agency is the successor to (a) the former National Security Service (which was previously part of the Ministry of Internal Affairs), (b) the division of that Ministry that is responsible for protecting the national communications infrastructure, (c) the military counterintelligence service of the Ministry of Defence, and (d) the former Financial Intelligence Agency.

42. The Agency is under the direct supervision of the government (section 2(1)). Its head is appointed by the President of the Republic, after being nominated the government, and his or her two deputies are appointed by the government (section 8(1) and (2)). The Agency's main tasks are to (a) safeguard national security from "encroachments directed against the national interests, independence and sovereignty of the Republic of Bulgaria, [its] territorial integrity, the fundamental rights and freedom of citizens, the democratic functioning of the State and the civic institutions, or the established constitutional order" (section 4(1)), and (b) carry out counterintelligence – in particular, for the protection of strategic installations (section 4(2) and (4)). It may be given other tasks only by [means of] statute (section 7).

43. It has, for instance, been given various tasks in relation to:

(a) money laundering and the financing of terrorism (sections 4, 4a, 5, 5b, 9, 9a, 9b, 9v, 11, 11a, 13-14a and 15 of the Measures Against Terrorist Financing Act 2003, and sections 8, 9e, 36a, 68, 71-79, 81-85, 87-94, 103-04, 108-09 of the Measures Against Money Laundering Act 2018);

(b) combatting terrorism (sections 8(1) of the Terrorism Countermeasures Act 2016);

(c) the acquisition of Bulgarian nationality (sections 33 and 35 of the Bulgarian Citizenship Act 1998, and section 41(1)(3) of the 2007 Act);

(d) security vetting for clearance to access certain types of classified information (sections 11, 12, 14, 48-49 of the Protection of Classified Information Act 2002);

(e) migration control and the expulsion and related detention of aliens (sections 22(4), 24c(17), 24i(11), 24i(6), 33h(1), 33kk(8), 33p(9), 42g and 44 of the Aliens Act 1998, and section 41(1)(2) and (2) and (3) of the 2007 Act);

(f) the granting of asylum or humanitarian protection (section 58(10) of the Refugees and Asylum Act 2002, and section 41(1)(1) of the 2007 Act);

(g) the protection of nuclear installations (sections 112-14 of the Peaceful Use of Nuclear Energy Act 2002); and

(h) cybersecurity (section 15 of the Cybersecurity Act 2018).

44. In 2013-15 the Agency also had the task of investigating criminal offences related to national security (section 4(6) of the 2007 Act, added in June 2013 and repealed in February 2015).

45. The Agency's two main areas of work are the gathering and analysis of intelligence (sections 18-20 and 28-29 of the 2007 Act). It can, in particular, engage in information analysis, forecasting and control (*прогностична [и] контролна дейност*), using its own information or information obtained from other authorities that is of importance for national security (section 4(3)). It may monitor people, objects and activities (section 5).

46. The Agency can, among other things, (a) carry out surveillance, (b) infiltrate agents in the course of its operations, and (c) use not-for-profit legal persons or commercial companies (section 20(1)(6), (1)(12) and (1)(20) of the 2007 Act). It can do all that through "specific methods and techniques", "special means of surveillance", and people collaborating with it (section 20(2)).

47. Section 21 of the 2007 Act specifies that the Agency has at its disposal and may deploy "special means of surveillance", under the conditions laid down in the 1997 Act (see paragraph 73 below).

B. "Agents on cover" used by the Agency

48. The 2007 Act mentions specifically the term "agents on cover" (*служители на прикритие*) in two provisions:

(a) section 35a, added in July 2018, which states that the Agency may refuse – in order to protect its intelligence-gathering methods or techniques – to disclose information about "agents on cover" or informers; and

(b) section 110(1)(7)(e), which has featured in the Act since its enactment in its original form, and according to which officers of the Agency who are "agents on cover" may be dismissed if they do not discharge their duties efficiently.

49. In addition, section 123(2)(6) of the 2007 Act – which has likewise in the Act since its enactment in its original form – states that the powers of the Agency comprise "organising the placing of Agency officers under cover (*прикриването на служители на агенцията*) and their work, featured under conditions and in a way laid down in regulations for the application of the Act".

C. Informers recruited by the Agency

50. The Agency may use informers (*сътрудници*), who must be protected in the course of or in connection with their collaboration (section 23(1) and (3)(2) of the 2007 Act). Their identities, personal data and work must be kept secret (section 23(3)(3)). Information about them may only be passed to the courts or the prosecuting authorities in connection with a specific criminal case, in keeping with the requirements of the Protection of Classified Information Act 2002 – and only after the informers in question have agreed to that (section 23(4)). The Agency may also withhold information about informers to protect its intelligence-gathering methods or techniques (section 35a).

D. Data processing by the Agency

51. The Agency may maintain and use databases (section 28(1) of the 2007 Act), and process information – including personal data (section 29(1) and (2)).

52. The Agency's databases may be automated (sections 34(1) and 36(2) of the 2007 Act). They may be used to process personal data (section 34(2)). The data controller is the head of the Agency, who may entrust the processing of personal data to designated officials (section 34(9)).

53. When processing personal data relating to any activities related to safeguarding national security, the Agency does not (a) seek the consent of the people concerned; (b) inform them before or during the processing; or (c) make available the personal data of other people (section 34(2)). Those

personal data are to be deleted if there is no longer any lawful reason for keeping them or if so ordered by a court (section 34(5)). The factors to be taken into account in that assessment comprise: the age of the individual concerned, the nature of the data being processed, the need to process them until the conclusion of a legal procedure or investigation, and the expiry of any statutory limitation period (section 34(6)). Personal data from the Agency's databases may be given only to the authorities safeguarding national security or the judicial authorities for the needs of a specific criminal case (section 34(7)). Those data may also be given to foreign authorities pursuant to an international treaty to which Bulgaria is party (section 34(8)).

54. Regulations issued by the head of the Agency in October 2019 pursuant to a statutory delegation in section 34(10) of the 2007 Act (*Наредба № I-4 от 22.10.2019 г. за реда за обработване на лични данни в Държавна агенция „Национална сигурност“*) lay down more detailed rules on the processing of personal data by the Agency. By regulation 2, that processing must be consistent with the principles of lawfulness, integrity, relevance and proportionality, and data security. By regulation 4, the head of the Agency: (a) fixes how the Agency creates, runs and controls databases containing personal data; (b) checks whether the processing of such data meets the requirements for its protection; (c) takes steps to rectify irregularities; and (d) assists the Commission for the Protection of Personal Data (see paragraphs 91-95 below) in the exercise of its supervisory functions under the Protection of Personal Data Act 2002 (see paragraphs 78-99 below). The head of the Agency (a) determines which Agency officers may process personal data (regulation 6(1)), and (b) decides, in each individual case, whether such data processed by the Agency is to be deleted, on the basis of a recommendation by the respective head of unit (regulation 17).

E. General supervision of the Agency's work

1. By Parliament

55. The Bulgarian Parliament (the National Assembly) has a special standing committee – the Committee for the Oversight of the Security Services, of the Application and Use of Special Means of Surveillance, and of Access to the Data under the Electronic Communications Act – which is tasked with, among other things, supervising the work of the Agency under: section 132(1) of the 2007 Act and section 22(1) of the Management and Functioning of the System for Protecting National Security Act 2015 ("the 2015 Act"); Rule 16 § 1 (11) of the 2021-22, 2022-23 and 2023-24 Rules of the National Assembly (which has been superseded by Rule 16 § 1 (10) of the 2024 Rules of the National Assembly); and Rule 4 of the latest (and nearly identical) iterations of the Committee's Rules, which were adopted in January 2022, November 2022, May 2023 and July 2024). In 2021-23, the Committee had fourteen members, and has since May 2023 had twelve members. The

Committee is reconstituted by each new Parliament. According to all of the successive decisions for its election (the latest ones were taken in December 2021, October 2022, May 2023 and July 2024), it must comprise members of Parliament from each parliamentary group. It must scrutinise, in particular, whether in their work the security services comply with the legal provisions guaranteeing basic human rights (Rule 15 § 1 (6) of the Committee's Rules). It can ask the security services to produce thematic reports (Rule 15 § 1 (4) of the Committee's Rules). It can also examine reports by individuals or organisations about misconduct by officers of the security services (Rule 15 § 1 (9) of the Committee's Rules), and refer unlawful conduct by those services that it has spotted in the course of its own inspections (or which have been complained of by individuals) to the prosecuting authorities or other competent authorities (Rule 15 § 1 (10) of the Committee's Rules).

56. The Agency's head, deputy heads and officers must appear before Parliament or the Committee if they are invited to do so, and make available to them any information that they are required to disclose (section 132(2) of the 2007 Act, section 22(2) of the 2015 Act, and Rule 15 § 1 (5) of the Committee's Rules). Section 22(2) *in fine* of the 2015 Act goes on to prescribe that this must be done in a manner that is consistent with the requirements of the Protection of Classified Information Act 2002.

2. By the Government

57. The head of the Agency presents to the government an annual report about the Agency's work, and the government then submits that report to the Parliament, which approves it (section 132(3) of the 2007 Act, and section 22(3) of the 2015 Act).

3. By the President of the Republic

58. The President of the Republic may require the head of the Agency to produce analyses of questions relating to national security (section 132a of the 2007 Act).

F. Access to personal data processed by the Agency

1. Relevant statutory provisions and regulations

59. Agency officers may not disclose information held by the Agency to other State authorities, organisations, legal persons or private persons except as prescribed by law (section 35(3)).

60. Anyone is entitled to request access to personal data that relate to him or her and are being processed in the Agency's databases without his or her knowledge (section 36(4)). The head of the Agency or a duly authorised deputy must respond to such a request within fourteen days of its being made (section 36(5)). If an individual asks, he or she must be given a paper copy of

any personal data relating to him or her that is being processed by the Agency (section 36(6)).

61. If the exercise of the right of access could reveal someone else's personal data, the data controller must give access only to those data that concern the individual requesting access (section 35(2)).

62. The exact manner of accessing the Agency's databases is prescribed in regulations made by its head (section 36(10)). Those regulations (*Наредба № I-7 от 13.07.2009 г. за реда за достъп до информационните фондове на Държавна агенция „Национална сигурност"*) were issued in 2009.

63. The Agency may refuse, wholly or in part, to disclose data if doing so would endanger national security, the protection of information classified as constituting a "State secret" or an "official secret", or the confidentiality of its sources of information or the covert methods and techniques that it uses to gather that information, or if disclosure would otherwise hinder the Agency's statutory tasks (section 36(7) and regulation 11(1)).

64. A person whose request has been refused must be advised of that in writing, but only the legal grounds for that refusal need to be given (section 36(8) and regulation 11(2)). The absence of a response within the time-limit is deemed to constitute a refusal (section 36(8) *in fine*).

65. Any such refusal is open to legal challenge under the relevant provisions of the Code of Administrative Procedure (section 36(9)) – in particular, by way of judicial review.

2. Case-law of the Bulgarian courts under those provisions

(a) 2012 case

66. In a 2012 judgment (*реш. № 593 от 08.02.2012 г. по адм. д. № 6653/2011 г., АдмС-София-град*) – which was apparently not appealed against – the Sofia City Administrative Court dismissed a claim for judicial review by a non-governmental organisation in respect of a refusal by the Agency to disclose how many such organisations it had investigated between January 2008 and July 2011, and what results any such enquiries had yielded. The court found, among other things, that information about the operations of the security services and their results was a "State secret", and on that basis held that the information sought by the organisation was classified. It went on to state that the disclosure of such information was also proscribed by section 36(7) of the 2007 Act (see paragraph 63 above).

(b) 2014-18 case

67. In a 2014 judgment (*реш. № 13080 от 04.11.2014 г. по адм. д. № 6237/2014 г., ВАС, V о.*), the Supreme Administrative Court set aside the tacit refusal of the Agency to disclose whether it was processing a certain person's data, and, if so, to give that person's access to any data pertaining to him that it was processing. The court held that in the absence of an express

decision taken by the Agency, there was no material indicating that any information regarding the data of the person in question had properly been withheld. It had to be ascertained in all such cases that the Agency, as a data controller, had duly assessed, with reference to the relevant rules (including section 36(7) – see paragraph 63 above), that the information in question ought not to be disclosed.

68. Following that judgment, the Agency expressly stated its refusal to disclose such information, stating that to do so would expose its sources and methods. The Varna Administrative Court dismissed the claim for judicial review of that decision, and in 2018 the Supreme Administrative Court upheld its judgment. It cited section 36(7) (see paragraph 63 above), and briefly noted that by section 3(1) of the Protection of Classified Information Act 2002, only people with security clearance who needed such classified information for their specific tasks could access it (see *реш. № 94 от 04.01.2018 г. по адм. д. № 5244/2016 г., ВАС, V о.*).

(c) First 2021-22 case

69. In a July 2021 judgment, the Sofia City Administrative Court dismissed a claim for judicial review of a refusal by the Agency to disclose whether it was processing a person's data and, if so, to afford her access to any of her personal data that it might be processing. The court noted that section 36(7) of the 2007 Act (see paragraph 63 above) listed five grounds on which the Agency could refuse to disclose information, and those included safeguarding "State secrets" and "official secrets", the sources of the information, and the covert methods or means for gathering it. The information sought by the claimant could be seen as constituting an "official secret". The Agency had discretion to assess whether disclosure of that information could expose classified information or harm its work. That was why section 36(8) of the 2007 Act (see paragraph 64 below) required the Agency to set out only the legal grounds for its refusal to disclose such information (see *реш. № 4760 от 16.07.2021 г. по адм. д. № 3553/2021 г., АдмС-София-град*). The appeal against that judgment was dismissed on procedural grounds, without reference to the merits, because it was defective and the claimant failed to rectify it within the time directed by the court (see *опр. № 3358 от 08.04.2022 г. по адм. д. № 798/2022 г., ВАС, V о.*).

(d) Second 2021-22 case

70. In a November 2021 judgment, the Sofia City Administrative Court dismissed a claim against a refusal by the Agency to disclose whether it had gathered intelligence on an association or its chairperson and whether it had recruited any of the association's members or staff as informers. The court gave almost exactly the same reasons as those that it had given in its July 2021 judgment (see paragraph 69 above) (see *реш. № 6820 от 19.11.2021 г.*

по адм. д. № 8299/2021 г., АС-София-град). In July 2022 the Supreme Administrative Court upheld that judgment. It held that the information request had in effect concerned the Agency's working methods rather than any personal data gathered by it, and went on to state that it had been proper for the Agency not to disclose who had been recruited by it as an informer, since, by section 23(3)(3) of the 2007 Act (see paragraph 50 *in fine* above) the identities and data of people who had collaborated with the Agency were to remain secret (see *реш. № 6724 от 06.07.2022 г. по адм. д. № 2157/2022 г., ВАС, V о.*).

(e) 2024 case

71. In a January 2024 judgment, the Sofia City Administrative Court quashed a second refusal by the Agency to disclose whether it had gathered intelligence on the same association or its chairperson and whether it had recruited any of the association's members or staff as informers. The court noted, in particular, that, in so far as the information request had concerned people other than the persons making it, it had been irregular, since one could seek access only to one's own personal data, and that the Agency should have therefore not have dealt with it on the merits (see *реш. № 136 от 05.01.2024 г. по адм. д. № 7471/2023 г., АдмС-София-град*). In July 2024 the Supreme Administrative Court upheld that ruling. It agreed with the reasons given by the lower court with respect to instances of a person seeking data relating to someone else, but added that under section 36(8) of the 2007 Act (paragraph 64 above) the Agency had no duty to set out the factual circumstances justifying a refusal by it to disclose information (see *реш. № 8858 от 16.07.2024 г. по адм. д. № 2605/2024 г., ВАС, V о.*). After the matter was then referred back to the Agency, in August 2024 it reiterated its earlier refusal, giving the same reasons, nearly word for word, that it had given in justifying that earlier refusal; in particular, it noted that under the relevant provisions of the Protection of Classified Information Act 2002 information that could lead to the identification of informers of the security services constituted a "State secret".

G. Supervision of the processing of personal data by the Agency

72. Section 37 of the 2007 Act, as originally enacted (and not amended since) provides that supervision of the protection of the rights of individuals in the course of the processing of their personal data by the Agency and of access to those data should be carried out by the Commission for the Protection of Personal Data, under the conditions and in the manner laid down by the Protection of Personal Data Act 2002 (see paragraphs 78-95 below).

II. SPECIAL MEANS OF SURVEILLANCE ACT 1997

73. A comprehensive account of the Special Surveillance Means Act 1997 ("the 1997 Act"), as amended, and related legislation – and of their application by the Bulgarian authorities and courts up until December 2021 – can be found in *Ekimdzhiev and Others v. Bulgaria* (cited above, §§ 11-145). That Act regulates in detail (a) the situations that may trigger the use of "special means of surveillance", (b) the persons who or objects which may be subjected to such surveillance, (c) the procedures for authorising such surveillance (which authorities may request it, how they must frame their requests, which authorities may issue surveillance warrants and how they must examine the requests for that the issuance thereof), (d) the maximum duration of such surveillance, (e) the situations in which such surveillance must be stopped, (f) the way in which information obtained through such surveillance is to be processed, and (g) the authorities supervising the use of "special means of surveillance".

74. By section 2(1) and (2) of the 1997 Act (and Article 172 § 1 of the Code of Criminal Procedure), the umbrella term "special means of surveillance" encompasses electronic or mechanical devices enabling the preparation of evidential material (video and audio recordings, photographs and marked objects) and the covert techniques employed in using those devices. By section 2(3) of the 1997 Act (and Article 172 § 1 of the Code), those techniques are (a) visual surveillance, (b) eavesdropping and tapping, (c) tracking, (d) covert intrusion (into vehicles or premises), (e) marking and checking correspondence or computerised information, (f) controlled delivery, (g) pseudo-transactions,[2] and (h) the use of "agents under cover" (*служители под прикритие*).

75. Sections 5-10c of the 1997 Act define each of those techniques. Under section 10c(1), an "agent under cover" is a public official serving in one of a number of specified law-enforcement authorities who is empowered to establish or maintain contacts with a "controlled person" to acquire or expose information about the commission of a serious wilful offence or the organisation of criminal activity. By Article 12b of the Criminal Code (which was added in 2010), an act committed by an "agent under cover" within the scope of his or her statutory powers is not an offence.

76. Under section 10c(2), the Agency may ask the Ministry of Internal Affairs to deploy an "agent under cover". Section 4 of the 1997 Act states, more generally, that "special means of surveillance" may be used in respect of activities relating to national security.

[2] Those also sometimes described as "simulated purchases" or "test purchases".

III. MANAGEMENT AND FUNCTIONING OF THE SYSTEM FOR SAFEGUARDING NATIONAL SECURITY ACT 2015

77. Section 2 of the Management and Functioning of the System for Safeguarding National Security Act 2015 defines "national security" as "a dynamic state of society and the State in which the territorial integrity, sovereignty and constitutional order are protected, and the democratic functioning of the institutions and the fundamental rights and freedoms of citizens are guaranteed, as a result of which the nation preserves and increases its welfare and develops, and the country successfully protects its national interests and realises its national priorities".

IV. PROTECTION OF PERSONAL DATA ACT 2002

78. The Protection of Personal Data Act 2002 ("the 2002 Act") was enacted to, among other things, ensure that Bulgaria would comply with its obligation under the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108; 1496 UNTS 65), which it had signed in 1998 and ratified in 2002, to take the necessary measures in its domestic law to give effect to the basic data protection principles.

79. As amended with effect from March 2019 with a view to (a) being brought into line with Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("General Data Protection Regulation" – "the GDPR"), and (b) transposing Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data ("Law Enforcement Directive" – "the LED"), the 2002 Act regulates all matters relating to the protection of personal data that are not set out in the GDPR itself (section 1(1)).

80. By paragraph 1(1) of the 2002 Act's additional provisions (as amended with effect from March 2019), "personal data" for the purposes of the Act has the meaning given to the term in Article 4(1) of the GDPR.[3]

[3] Article 4(1) of the GDPR defines "personal data" as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

A. Scope of application

1. Ratione personae

81. The provisions of the 2002 Act, irrespective of whether they concern the processing of personal data falling within the scope of the GDPR or the processing of such data by the authorities for law-enforcement purposes, apply only to data relating to individuals (that is, natural persons) (section 1(1) and (2)).

2. Application to processing for national security purposes

82. The 2002 Act, as worded since March 2019, does not apply to the processing of personal data for national security purposes, unless that is expressly provided for elsewhere (section 1(5)). The explanatory notes to the government bill (no. 802-01-27) which led to the March 2019 amendments to the Act (see paragraph 78 above) stated that section 1(5) had been put in place to reflect the position that the GDPR and the LED did not apply to the processing of personal data for activities falling outside the scope of European Union (EU) law. In a November 2023 judgment (*реш. № 10522 от 02.11.2023 г. по адм. д. № 140/2023 г., ВАС, V о.*), the Supreme Administrative Court pointed out that national security purposes within the meaning of section 1(5) were to be distinguished from law-enforcement purposes.

83. When originally enacted, the 2002 Act stated that the processing of personal data for national security purposes could be governed by a special statute (section 1(4), as worded in 2002-05). In 2005 that subsection was amended to provide that such processing was to be governed by a special statute (section 1(4), as worded in 2005-06). In late 2006 section 1(4), which became section 1(5), was amended once more – this time to state that the Act did apply to the processing of personal data for national security purposes unless a special statute provided otherwise (section 1(5), as worded in 2006-19).

84. During that period, in 2014, the authority in charge of supervising the application of the 2002 Act, the Commission for the Protection of Personal Data (see paragraph 91 below), received a complaint by an individual suspecting that the Agency had covertly intercepted his telephone communications. He had asked the Agency for information on the point under the 2002 Act, and the Agency had refused to give it, saying that it fell outside the scope of that Act. He then complained of that refusal to the Commission, which dismissed his complaint, agreeing that the information which he had sought from the Agency fell outside the scope of the 2002 Act as it did not concern personal data. According to the Commission, information about the use of "special means of surveillance" could be sought only from the body

supervising the use of such means – the National Bureau for the Oversight of Special Means of Surveillance (see *реш. № Ж-780 от 08.10.2014 г., КЗЛД*).

B. Right to access personal data and restrictions to that right

1. In relation to processing falling within the scope of the GDPR

85. The right of access to information whose processing falls within the scope of the GDPR is governed by its Article 15(1)(a), according to which a "data subject is entitled to obtain from the controller confirmation whether personal data concerning him or her are being processed, and, if that is so, access to those data and information about the purposes of their processing".

86. A data controller or processor may restrict, wholly or in part, the data subject's access or other rights under Articles 12-22 of the GDPR if their exercise would create a risk for national security (section 37a(1)(1) of the 2002 Act, which reflects Article 23(1)(a) of the GDPR). Section 37a(2) specifies that the way in which this can be done must be prescribed by law and consistent with Article 23(2) of the GDPR.

2. In relation to processing by the authorities for law-enforcement purposes

87. A data subject is entitled to obtain from the controller confirmation of whether personal data concerning him or her are being processed, and (if they are) access to those data and to information about the purposes of their processing (section 55(1)(1) read in conjunction with section 54(1)(5) and (2)(1) of the 2002 Act, which transposed Article 14 (a) of the LED).

88. Those rights may be restricted wholly or in part if that is necessary to, among other things, safeguard national security – so long as due regard is paid to the fundamental rights and legitimate interests of the persons concerned (section 55(3) read in conjunction with section 54(3)(4) of the 2002 Act, which implemented the exemption permitted by Article 15(1)(d) of the LED). When the obstacle ceases to exist, the data controller must normally provide that information within two months of it being requested by the data subject (section 55(3) *in fine* read in conjunction with sections 54(4) and 53(3)).

89. If access to personal data is refused or restricted under the above-noted provisions, the data controller must inform the data subject of that refusal or the restriction (and of the reasons therefor) within two months, but may omit to do so if that would defeat the purpose of those measures (section 55(4) read in conjunction with section 53(3) of the 2002 Act, which transposed Article 15(3) of the LED). In that event, the data controller must nonetheless record the factual and legal reasons on which that decision rests, and make them available to the competent supervisory authority – which is, in most cases, the Commission for the Protection of Personal Data, whose tasks and

powers are set out in paragraphs 91-95 below (section 55(5) of the 2002 Act, which transposed Article 15(4) of the LED).

90. If such restrictions have been put in place by a data controller that is not a court or a prosecuting or investigating authority,[4] the data subject may exercise his or her right of access under section 55(1) of the 2002 Act indirectly, through the Commission for the Protection of Personal Data. If the data subject does so, that Commission must check the lawfulness of the restriction (section 57(1) of the 2002 Act, which transposed Article 17(1) of the LED), and inform the data subject at least that all necessary verifications or a review have taken place (section 57(2) of the 2002 Act, which transposed Article 17(3) of the LED).

C. Supervisory authority

91. The Commission for the Protection of Personal Data supervises the processing of personal data falling within the scope of the GDPR, as well as such processing for law-enforcement purposes by all authorities, except the courts and the prosecuting and investigating authorities (sections 6(1), 10(1), 10a(1) and 78 of the 2002 Act).[5]

92. In carrying out that supervision, that Commission must, among other things, (a) handle complaints by data subjects, (b) check the lawfulness of the processing in cases in which the data subject's access right has been restricted (see paragraphs 88 and 90 above), and (c) inform the data subject within three months of the outcome of that verification or of the reasons for it not being carried out (Article 57(1)(f) of the GDPR and section 79(1)(5) and (1)(6) of the 2002 Act, which transposed Article 46(1)(f) and (g) of the LED).

93. When supervising data processing for law-enforcement purposes, that Commission may obtain from the controller or the processor access to (a) all personal data being processed and (b) all the information necessary for it to carry out its tasks (section 80(1)(1) and (1)(2) of the 2002 Act, which transposed Article 47(1) of the LED).

94. When supervising data processing for law-enforcement purposes, that Commission may (a) order the controller or processor to bring processing operations into compliance with the relevant part of the 2002 Act – in particular, by ordering the rectification or erasure of personal data or the restriction of their processing, pursuant to section 56 of the Act, and (b) impose a temporary or definitive limitation, including a ban, on processing (section 80(1)(3) and (1)(4)) of the 2002 Act, which transposed Article 47(2)(b) and (c) of the LED). The Commission has exercised those

[4] The processing of personal data for law-enforcement purposes by the courts and by the prosecuting and investigating authorities (which by Article 117 § 2 of the 1991 Constitution of Bulgaria are also part of the judicial branch) is supervised by the Supreme Judicial Council's Inspectorate (section 78(2) of the 2002 Act).

[5] See footnote 3 above.

powers on at least three occasions with respect to the Ministry of Internal Affairs (see *реш. № ППН-01-482/2020 от 10.05.2021 г., КЗЛД*; *реш. № ППН-01-361/2021 от 18.01.2022 г., КЗЛД*; and *реш. № ППН 01-350/2021 от 17.03.2022 г., КЗЛД*).

95. That Commission may also bring infringements of the relevant part of the 2002 Act to the attention of the courts (section 80(3) of the 2002 Act, which transposed Article 47(5) of the LED).

96. In its annual report for 2009, that Commission recorded, on page 28, that it had entered into a cooperation agreement with the Agency for the purpose of realising closer collaboration between the two in the area of personal-data protection (in a spirit of respect for each other's independence and respective areas of responsibility); that cooperation encompassed the coordination, exchange, holding and use of data and information, as well as the creation of joint working groups and the provision of expert or technical assistance. The Commission also noted, on page 35 *in fine*, that it was about to finalise an audit of the Agency in connection with preparations for the future implementation of the Schengen Information System. In its annual report for 2010, the Commission recorded, on page 38, that it had continued its cooperation with the Agency pursuant to the agreement made in 2009. In its annual report for 2015, the Commission referred, on pages 42-43, to a check on a private foundation that it had carried out together with other authorities, including the Agency. In its annual report for 2016, the Commission referred, on pages 98-99, to its cooperation with the Agency regarding the transposition of new legislation (for instance, regarding the creation of a new financial-intelligence unit within the Agency) and international cooperation. The Commission has not mentioned, in any of its annual reports for the period 2009-23, any inspections which it has carried out in the Agency apart from the above-mentioned 2009 audit relating to the future implementation of the Schengen Information System.

D. Remedies

1. In respect of processing falling within the scope of the GDPR

97. Data subjects considering that their rights under the GDPR or the 2002 Act have been breached may complain to the Commission for the Protection of Personal Data, and seek judicial review of its decision (section 38(1) and (7) (since May 2023 subsection (8)) of the 2002 Act, which reflects Articles 77(1) and 78(1) and (2) of the GDPR).

98. Data subjects may also directly seek judicial review of actions undertaken or decisions issued by the data controller or processor, or damages from them, if the data controller or processor have processed their personal data unlawfully (section 39(1) and (2) of the 2002 Act, which reflects Articles 79(1) and 82(1) of the GDPR).

2. In respect of processing by the authorities for law enforcement purposes

99. The remedies for alleged breaches of the rights of data subjects that occur in the course of the processing of personal data by the authorities for law-enforcement purposes are the same as those for alleged breaches in the course of processing that fall within the scope of the GDPR (section 82(1) of the 2002 Act, which transposed Articles 52(1), 53 and 54 of the LED).

V. CODE OF ADMINISTRATIVE PROCEDURE

100. By Article 150 § 1 (5) of the 2006 Code of Administrative Procedure, a claim for judicial review must indicate the administrative decision against which it is directed.

THE LAW

I. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

101. The applicant association complained that the 2008 regulations permitting the use of "agents on cover", as amended in 2018, fell short of the requirements of Article 8 of the Convention in various respects, especially in terms of safeguards, and thus enabled the Agency to deploy such agents in an arbitrary and abusive manner – in particular given that the regulations, which made no provision for the persons concerned to be notified of the Agency's decision to deploy such agents, did not make it possible to challenge that decision. In that latter respect, the association relied also on Articles 6 § 1 and 13 of the Convention.

102. In the light of the Court's case-law in relation to matters of the kind in issue in the present case (see *Roman Zakharov v. Russia* [GC], no. 47143/06, § 307, ECHR 2015; *Centrum för rättvisa v. Sweden* [GC], no. 35252/08, § 377, 25 May 2021; *Ekimdzhiev and Others v. Bulgaria*, no. 70078/12, § 247, 11 January 2022; and *Pietrzak and Bychawska-Siniarska and Others v. Poland*, nos. 72038/17 and 25237/18, § 127, 28 May 2024; see also, *mutatis mutandis*, *Brito Ferrinho Bexiga Villa-Nova v. Portugal*, no. 69436/10, §§ 33-35, 1 December 2015), and in view of the way in which the association formulated its complaint, it falls to be examined solely under Article 8 of the Convention. That Article reads, so far as relevant:

> "1. Everyone has the right to respect for his private ... life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

A. Admissibility

1. The parties' submissions

(a) Victim status

103. The Government's submissions on this point, which they framed in terms of the existence of an interference with the association's rights under Article 8 of the Convention, have been set out in paragraphs 110-111 below (see, for a similar approach, *Fu Quan, s.r.o. v. the Czech Republic* [GC], no. 24827/14, § 88 *in fine*, 1 June 2023).

104. The applicant association submitted that it suspected that the Agency had infiltrated "agents on cover" in it, since that was fully possible under the regulations in issue. The Agency was under no duty to notify the association of that, and there was no lawful way for the association to learn whether that had happened; the Government had not denied it in their observations.

(b) Exhaustion of domestic remedies

105. The Government argued that domestic remedies had not been exhausted, on the basis that the association's members could have sought access to personal data relating to them and processed in the Agency's databases under section 36(4) of the 2007 Act (see paragraph 60 above), and challenged before the administrative courts any refusal by the Agency to give such access under section 36(9) of the same Act. That possibility was still open, and could enable the association to ascertain whether the Agency had indeed gathered information about itself or its members.

106. The applicant association replied that by pursuing to a conclusion the proceedings for judicial review of the impugned regulations, it had exhausted domestic remedies.

2. The Court's assessment

(a) Victim status and exhaustion of domestic remedies

107. The question of whether the applicant association can claim to be victim of interference with its rights under Article 8 of the Convention on account of the mere existence of the regulations in issue and whether it has exhausted domestic remedies is closely bound up with the substance of the complaint. The Government's non-exhaustion objection and their objection that the association cannot claim to be a victim must, then, be joined to the merits (see, *mutatis mutandis*, *Roman Zakharov*, § 150; *Ekimdzhiev and Others*, § 259; and *Pietrzak and Bychawska-Siniarska and Others*, § 129, all cited above).

(b) Conclusion about the admissibility of the complaint

108. The complaint is, moreover, not manifestly ill-founded or inadmissible on other grounds. It must therefore be declared admissible.

B. Merits

1. Victim status and the existence of an interference with rights protected under Article 8 of the Convention

(a) The parties' submissions

(i) The applicant association

109. The applicant association submitted that the mere existence of the regulations, which enabled the Agency to infiltrate "agents on cover" in private organisations, amounted to interference with its rights under Article 8 of the Convention. In its view, the distinction between "agents under cover" and "agents on cover" was "mere wordplay" and did not reflect any substantive difference, since "agents on cover" could equally encroach on the home or communications of the organisations into which they could be infiltrated – even if they used no technical means to do so.

(ii) The Government

110. The Government argued that it followed from *Lüdi v. Switzerland* (15 June 1992, § 40, Series A no. 238) that the use of covert operatives did not necessarily affect "private life" or "correspondence". They also submitted that the work of "agents on cover" did not lead to an intrusion into the private sphere of the same sort, in terms of degree and probability of occurrence, as that entailed by covert surveillance measures such as the interception of communications. The role of "agents on cover" was merely to ascertain criminal conduct that would have taken place in any case.

111. The Government also submitted that the association's complaint was wholly abstract, since it did not allege that it had been infiltrated by "agents on cover". In their view, the specific nature of "agents on cover" meant that the Court's approach to the question of whether someone could claim to be victim of interference with rights guaranteed by Article 8 of the Convention by reason of the mere existence of a law permitting covert surveillance could not be readily transposed to "agents on cover". It was essential in that connection to highlight the difference between "agents under cover" and "agents on cover". In Bulgaria, the former constituted a type of "special means of surveillance" that were subject to the provisions of the 1997 Act (see paragraphs 73-75 above), whereas the latter were not. They could not give evidence in criminal proceedings, or use technical means to record anything or produce material for use in such proceedings. Their work did not entail any active investigation; it was passive. They operated under their real names, and were not exempt from criminal or civil liability. A report by an

"agent on cover" to the relevant authority about an offence was no different from the report that any member of the public had the legal duty to make. The work of "agents on cover" could therefore not be seen as interference with the association's "private life" or "correspondence".

(b) The Court's assessment

112. The issue of whether the existence of the regulations in issue – which enable the Agency to deploy "agents on cover" in private organisations – interferes with rights of the applicant association under Article 8 of the Convention comprises two questions. The first is whether the work of an "agent on cover" can, in view of its characteristics, in principle interfere with such rights. If the answer to that first question is yes, the second question is whether the association can claim to be a victim of such interference on account of the mere existence of those regulations.

(i) Could the work of an "agent on cover" interfere with the rights of the applicant association under Article 8 of the Convention?

113. An "agent on cover" infiltrated into the association would undoubtedly be able to obtain data about the association's "correspondence" within the meaning of Article 8 § 1 of the Convention (see, *mutatis mutandis*, *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, no. 62540/00, § 60, 28 June 2007, and *Ekimdzhiev and Others*, cited above, § 263). As construed in the Court's case-law, that term covers all sorts of private communications, whatever their content or the form that they might take – oral communications, letters, telephone conversations or electronic exchanges (see *Michaud v. France*, no. 12323/11, § 90, ECHR 2012; *M.N. and Others v. San Marino*, no. 28005/12, § 52, 7 July 2015; and *Klaus Müller v. Germany*, no. 24173/18, § 37, 19 November 2020). In particular, it comprises calls made from, or received on, office telephones (see *Halford v. the United Kingdom*, 25 June 1997, § 44, *Reports of Judgments and Decisions* 1997-III; *Kopp v. Switzerland*, 25 March 1998, § 50, *Reports* 1998-II; *Amann v. Switzerland* [GC], no. 27798/95, § 44, ECHR 2000-II; *Liblik and Others v. Estonia*, nos. 173/15 and 5 others, § 110, 28 May 2019; and *Algirdas Butkevičius v. Lithuania*, no. 70489/17, § 63, 14 June 2022), as well as work emails (see *Copland v. the United Kingdom*, no. 62617/00, § 41, ECHR 2007-I). The term "correspondence" also covers the communications of legal persons (see *Ships Waste Oil Collector B.V. and Others v. the Netherlands* [GC], nos. 2799/16 and 3 others, § 146, 1 April 2025).

114. It should be noted in this connection that, as borne out by the facts of many cases examined by the Court, "correspondence" can be interfered with not only at the time when it is being sent or received, but also subsequently, through accessing the medium – physical or electronic – where it has been stored (see *Niemietz v. Germany*, 16 December 1992, § 32,

Series A no. 251-B; *Wieser and Bicos Beteiligungen GmbH v. Austria*, no. 74336/01, § 45, ECHR 2007-IV; *Bernh Larsen Holding AS and Others v. Norway*, no. 24117/08, § 106, 14 March 2013; *Vinci Construction and GTM Génie Civil et Services v. France*, nos. 63629/10 and 60567/10, § 63, 2 April 2015; *M.N. and Others v. San Marino*, cited above, §§ 54-55; *Sérvulo & Associados – Sociedade de Advogados, RL and Others v. Portugal*, no. 27013/10, § 76, 3 September 2015; *Saber v. Norway*, no. 459/18, § 48, 17 December 2020; *Särgava v. Estonia*, no. 698/19, § 85, 16 November 2021; and *Naumenko and SIA Rix Shipping v. Latvia*, no. 50805/14, § 45, 23 June 2022).

115. It is not far-fetched to surmise that (a) a covert operative infiltrated into an organisation could use his or her position to obtain such access in a manner that would not be possible for an outsider, and that (b) such an operative, being an Agency officer, would report his or her findings to the Agency far more readily, and in a more sustained and systematic way, than a member of the public or a whistleblower driven by a sense of civic duty or even by statutory duty.

116. The infiltration of an "agent on cover" into the association would therefore amount to interference with its right to respect for its "correspondence" within the meaning of Article 8 § 1 of the Convention.

117. An "agent on cover" infiltrated into the association would also be likely to have long-term access to its office or other premises. According to the Court's case-law, a legal person's registered office, branches and other business premises can be considered as that legal person's "home" within the meaning of Article 8 § 1 of the Convention (see *Société Colas Est and Others v. France*, no. 37971/97, § 41, ECHR 2002-III; *Buck v. Germany*, no. 41604/98, § 31, ECHR 2005-I; *Sallinen and Others v. Finland*, no. 50882/99, § 70, 27 September 2005; *Heino v. Finland*, no. 56720/09, § 33, 15 February 2011; *Bernh Larsen Holding AS and Others*, cited above, § 104; *Saint-Paul Luxembourg S.A. v. Luxembourg*, no. 26419/10, § 37, 18 April 2013; *DELTA PEKÁRNY a.s. v. the Czech Republic*, no. 97/11, § 77, 2 October 2014; *Lindstrand Partners Advokatbyrå AB v. Sweden*, no. 18700/09, § 83, 20 December 2016; and *Ships Waste Oil Collector B.V. and Others*, cited above, § 146; see also *Naumenko and SIA Rix Shipping*, cited above, § 46, and *UAB Kesko Senukai Lithuania v. Lithuania*, no. 19162/19, § 109, 4 April 2023).

118. The infiltration of an "agent on cover" into the association would therefore also amount to interference with its right to respect for its "home" within the meaning of Article 8 § 1 of the Convention.

119. In view of the conclusions set out in paragraphs 116 and 118 above, it would be superfluous to ascertain whether the use of an "agent on cover" with respect to the association would also amount to interference with its right to respect for its "private life", if any (in relation to individuals, see on the one hand, *Lüdi*, cited above, § 40, and, on the other, *Verliere v. Switzerland*

(dec.), no. 41953/98, ECHR 2001-VII, and *Vukota-Bojić v. Switzerland*, no. 61838/10, § 59, 18 October 2016; in relation to legal persons, see *Bernh Larsen Holding AS*, cited above, § 107).

(ii) Can the applicant association claim to be a victim of interference with those rights on account of the mere existence of the regulations on "agents on cover"?

(α) General principles

120. The previously diverging strands of case-law regarding when applicants could claim to be victims of interference with their rights under Article 8 of the Convention on account of the mere existence of domestic laws or practices permitting covert surveillance were harmonised, and the general principles on the point clarified, in *Roman Zakharov* (cited above, § 171). They were more recently restated in *Centrum för rättvisa* (cited above, § 167).

121. Those principles are equally relevant to situations, such as the one at hand, where the secrecy of the surveillance in question is achieved not through fully disguising from the target that monitoring is under way – as happens for instance with the covert interception of communications or the use of covert surveillance equipment such as hidden cameras or recording devices – but through systematic arrangements calculated to conceal simply that the target's otherwise overt interlocutor (an acquaintance, business contact, employee, colleague, service provider, client, fellow practitioner, and so on) is in fact an operative systematically using or manipulating his or her position or relationships to obtain information for use by the authorities. In such situations, the persons targeted or affected by such surveillance remain similarly unaware of it.

(β) Application of those principles

– *Scope of the relevant law*

122. Under the terms of regulation 52(1) of the 2008 Regulations, "agents on cover" may be deployed if there is a "proven operational need", and, by regulation 53(1) and (2), they can carry out intelligence and counterintelligence work aimed at the protection of national security, and their specific tasks are to be set by the head of the Agency in each individual case (see paragraphs 11-12 above). By regulation 50, as amended in September 2018, "agents on cover" can be infiltrated into any private organisation (see paragraphs 28-29 above). It follows that, theoretically, any non-governmental organisation in Bulgaria can become the target of such measures, and thus possibly be affected by the regulations in issue.

– *Availability of an effective remedy*

123. The next question is whether there exists in Bulgaria an effective remedy that can alleviate suspicions among the general public that the Agency's capability to deploy "agents on cover" can be abused.

124. As repeatedly insisted upon at the domestic level and by the Government in their observations before the Court (see paragraphs 24, 32-33, 36, 39-40 and 111 above), "agents on cover" do not constitute "special means of surveillance" within the meaning of the 1997 Act and related legislation (see paragraph 74 above). It follows that the body supervising the use of "special means of surveillance" in Bulgaria – the National Bureau for the Oversight of Special Means of Surveillance – is under no duty to supervise the deployment of such agents or to inform the persons concerned that such agents have been used with respect to them (see *Ekimdzhiev and Others*, cited above, §§ 130-35). It also follows that the special remedy put in place in 2009 with respect to "special means of surveillance" – a claim for damages in respect of their unlawful use (ibid., §§ 136-44 and 265-72) – does not apply to "agents on cover". That remedy is, in any event, not open to legal persons such as the applicant association (ibid., § 273). Indeed, the Government did not seek to argue that those legal avenues could provide any redress with respect to the use of "agents on cover".

125. What the Government did suggest was that members of the applicant association could have sought access to personal data of theirs processed in the Agency's databases by way of a request lodged under section 36(4) of the 2007 Act (see paragraph 60 above), and then challenged before the administrative courts under section 36(9) any refusal by the Agency to afford access to such data (see paragraph 105 above) – and thus discovered information about any "agents on cover" used with respect to the association.

126. Leaving to one side the fact that this avenue was not open to the association itself (since it is a legal person), it does not appear that that course of action was in practice capable of providing information about the use of "agents on cover" by the Agency. According to section 36(7) of the 2007 Act, the Agency can refuse, wholly or in part, to disclose data sought under section 36(4) if doing so would endanger national security, the protection of information classified as constituting a "State secret" or "official secret", or the confidentiality of its sources of information or of the covert methods and techniques employed by it in gathering that information, or if such disclosure would otherwise hinder the Agency's statutory tasks (see paragraph 63 above). Moreover, under section 35a of the 2007 Act, the Agency may refuse to disclose information about "agents on cover" to protect the methods or techniques that it uses to gather intelligence (see paragraph 48 (a) above). All examples of requests lodged under section 36(4) and ensuing judicial review challenges under section 36(9) of which the Court is aware, spanning over the period 2012-24, show that the Agency has been systematically availing itself of the possibility to refuse to disclose information about any aspect of

its operations and that the Bulgarian administrative courts have been consistently upholding those refusals (see paragraphs 66-71 above; also compare, *mutatis mutandis*, *Pietrzak and Bychawska-Siniarska and Others*, cited above, § 241). The Government have not cited any contrary examples.

127. It follows that the remedy under section 36(4) and (9) of the 2007 Act cannot sufficiently dispel the public's misgivings about the threat posed by the abusive deployment of "agents on cover" by the Agency. It also follows that the Government's non-exhaustion objection based on those provisions (which was joined to the merits – see paragraphs 105 and 107 above) must be dismissed.

128. Nor can those misgivings be dispelled by other possible remedies.

129. The Government did not argue – and there is no indication – that there have so far been any instances of someone being able to obtain information concerning, or redress in relation to, the use of an "agent on cover" by way of lodging a complaint with the Commission for Protection of Personal Data. It is true that section 37 of the 2007 Act empowers that Commission to supervise the processing of personal data by the Agency in the manner provided by the 2002 Act (see paragraph 72 above). At the same time, section 1(5) of the 2002 Act itself (as amended in March 2019) states that the 2002 Act does not apply to the processing of personal data for national security purposes unless such processing is expressly provided for elsewhere – the stated rationale being that the elaborate data protection regime instituted by EU law, especially since the adoption of the GDPR and the LED, and reflected in the 2002 Act – does not cover the processing of personal data for activities relating to the protection of national security (see paragraph 82 above). It is therefore unclear whether section 37 of the 2007 Act can be read to mean that the 2002 Act's strictures apply to the processing of such data by the Agency for operational purposes (or only for other purposes – such as, for instance, staff administration and public procurement), and that that Commission can exercise the investigatory and remedial powers that it has under the 2002 Act with respect to data obtained by the Agency in the course of its intelligence operations.

130. Nor is there any indication that – apart perhaps from a 2009 audit of the Agency in connection with preparations for the future implementation of the Schengen Information System – that Commission has ever checked how the Agency processes operational data – and, in particular, whether it duly follows the statutory rules and the regulations which govern that matter (see paragraphs 52-54 and 96 above; also compare *Ekimdzhiev and Others*, cited above, §§ 346 and 412; also contrast, *mutatis mutandis*, *Centrum för rättvisa*, cited above, § 351, and *Big Brother Watch and Others v. the United Kingdom* ([GC], nos. 58170/13 and 2 others, §§ 409-10, 25 May 2021). On the contrary, the (apparently) only case in which that Commission was invited to look into the matter indicates that it was of the view that data resulting from surveillance carried out by the Agency did not amount to personal data, and

that such operations by the Agency were not for it to supervise (see paragraph 84 above).

131. The possibility of complaining to that Commission cannot therefore be seen as an effective remedy with respect to the use of "agents on cover" (compare, *mutatis mutandis*, *Ekimdzhiev and Others*, cited above, § 346, and *Hüttl v. Hungary* [Committee], no. 58032/16, §§ 15-18, 29 September 2022; also contrast *Breyer v. Germany*, no. 50001/12, §§ 105 and 107, 30 January 2020, and *Ringler v. Austria* (dec.) [Committee], no. 2309/10, §§ 72-79, 15 May 2020).

132. The same considerations apply to the other general data protection remedies under the 2002 Act (see paragraphs 97-99 above).

133. The general possibility of seeking judicial review of the decisions of the head of the Agency – to which the Government referred in their observations on the merits (see paragraph 137 (b) below) – cannot be seen as an effective remedy with respect to the use of "agents on cover" either. The persons targeted or affected (whether directly or collaterally) by the deployment of such agents are by definition unaware that such deployment has taken place. As the Court has consistently emphasised, there is little scope for recourse to the courts unless those concerned are advised of a measure taken without their knowledge and are thus able to challenge it (see *Klass and Others v. Germany*, 6 September 1978, § 57, Series A no. 28; *Weber and Saravia v. Germany* (dec.), no. 54934/00, § 135, ECHR 2006-XI; *Roman Zakharov*, cited above, § 234; *Sommer v. Germany*, no. 73607/13, § 62, 27 April 2017; *Centrum för rättvisa*, cited above, § 251; and *Big Brother Watch and Others*, cited above, § 337). The Government have not sought to argue that such a claim for judicial review can be brought blindly, without identifying the specific decision of the head of the Agency that is being challenged – which is a general requirement for claims for judicial review in Bulgaria (see paragraph 100 above; also contrast, *mutatis mutandis*, *Big Brother Watch and Others*, cited above, § 413).

134. Seeking to engage the personal liability of "agents on cover" for acts carried out in the course of their work – a possible remedy to which the Government also referred in their observations on the merits (see paragraph 137 (c) below) – cannot be seen as an effective remedy with respect to the use of such agents either. There is an air of unreality about the suggestion that it is possible to engage the personal liability of such agents for unlawful interferences with rights protected under Article 8 of the Convention during the course of their work in the absence of any lawful possibility for the persons affected by their deployment to learn about it. Moreover, according to the Court's case-law, suing a private person does not constitute a remedy in respect of acts of the State (see *Pine Valley Developments Ltd and Others v. Ireland*, 29 November 1991, § 48, Series A no. 222; *Iatridis v. Greece* [GC], no. 31107/96, § 47 *in fine*, ECHR 1999-II; and *Zlínsat, spol. s r.o., v. Bulgaria*, no. 57785/00, § 55 *in fine*, 15 June 2006).

– *Conclusion*

135. For the above reasons, the mere existence of the regulations in issue – which have since September 2018 permitted the infiltration of "agents on cover" into private organisations – can be seen as interference with the applicant association's rights under Article 8 of the Convention, without it being necessary to ascertain whether the association is at risk of having such agents infiltrated into it owing to its specific situation. It is therefore justified to examine those regulations (along with any related laws and practices) in the abstract (see, *mutatis mutandis*, *Centrum för rättvisa*, cited above, §§ 175-76). Indeed, by pursuing to a conclusion its claim for judicial review of those regulations (see paragraphs 31-40 above), the association has exhausted the available domestic remedies in respect of its complaint on that point. It follows that the Government's objection that the association cannot claim to be a victim of interference with its Article 8 rights, which was – like their non-exhaustion objection – joined to the merits (see paragraphs 103 and 107 above), must be dismissed.

2. *Justification for the interference*

(a) The parties' submissions

(i) The applicant association

136. The applicant association submitted that the interference had been neither "in accordance with the law" nor "necessary in a democratic society", since the regulations, which lacked detail and were unclear, did not lay down any safeguards against the misuse of "agents on cover". No conditions restricted their use, and they could be resorted to whenever the Agency deemed that there was an operational need for so doing. Nor was their use subject to prior authorisation or subsequent supervision by a judge. That opened the way towards their arbitrary deployment. Moreover, no rules defined their work, and no time-limits or procedures constrained their deployment. It seemed as though the very concept "of "agents on cover" had been devised to circumvent the statutory limitations on deploying "agents under cover". It was impossible in practice to engage the liability of such "agents on cover" in respect of any unlawful acts, since their identities remained confidential.

(ii) The Government

137. The Government argued that the preconditions for the use of "agents on cover" under the regulations in issue indicated that such agents were to be used exceptionally and as a measure of last resort, and emphasised in that connection the need for States to safeguard their national security. They also pointed out that the tasks of "agents on cover" were specifically set in each case, and argued that that their deployment was not without supervision, since

(a) the Agency's work was supervised by Parliament, the President of the Republic and the Government, (b) all decisions of the Agency's head could be subjected to judicial review, and (c) "agents on cover" bore civil and criminal liability in respect of any unlawful acts carried out in the course of their work. Moreover, such agents had to apply for the position in which they would be infiltrated just like any other person, and needed to have the requisite qualifications to fill any such position. That meant that the Agency was not able to uncontrollably infiltrate such agents into any legal entity. Nor could those agents use technical means to record anything. Their work had a merely informative character and did not entail active investigation.

138. The Government went on to argue that the relevant law was fully accessible, since the 2007 Act and the impugned regulations had been published in the State Gazette. Moreover, the preconditions for infiltrating an "agent on cover" laid down in those regulations – in particular, that the use of such agents was a means of last resort and that they could be deployed only if there was a "proven operational need" – and the way in which they were to be infiltrated ensured that their use would be proportionate to the specific aims which called for it. As regards specifically the term "national security", it had been defined by statute (see paragraph 77 above). In the light of all those factors, it could also be accepted that the alleged interference had been intended to safeguard national security and to prevent disorder and crime, that "agents on cover" would not be used if that was not "necessary in a democratic society", and that the proportionality of resorting to them would be ascertained in each individual case.

139. The absence of time-limits in respect of the deployment of "agents on cover" was not an issue, since those were difficult to fix in advance. Nor could it be required that the authorities notify a target person or entity that an "agent on cover" has been deployed against him, her or it, since that could frustrate the purpose of using an "agent on cover". Those concerned by such a measure could seek information about the use of such agents under section 36(4) of the 2007 Act (see paragraph 60 above), and in such event the Agency would decide, with reference to the criteria in section 35a (see paragraph 48 (a) above), whether to give such information.

(b) The Court's assessment

140. Under the second paragraph of Article 8 of the Convention, an interference with the rights protected by that Article can be justified only if it is "in accordance with the law" and "necessary in a democratic society" to attain one or more of the legitimate aims set out in that paragraph. Such interference otherwise entails a breach of that Article.

(i) General principles

(α) With regard to the level of safeguards

141. The general principles regarding when covert surveillance can be justified under Article 8 § 2 of the Convention were set out in detail in *Roman Zakharov* (cited above, §§ 227-34, 236, 243, 247, 250, 257-58, 275, 278 and 287-88). Many of those principles were more recently reiterated, although in relation to a somewhat different context – the bulk interception of communications – in *Centrum för rättvisa* (cited above, §§ 246-53) and *Big Brother Watch and Others* (cited above, §§ 332-39).

142. There is no need to repeat those principles in full here, except to emphasise that the overarching requirement is that any covert surveillance system must contain effective safeguards – especially review and supervision arrangements – which can protect against the inherent risk of arbitrariness and abuse, and which can keep the interference that such a system entails with the rights protected by Article 8 of the Convention to what is "necessary in a democratic society".

143. Those principles are equally relevant to situations, such as the one at hand – where, as noted in paragraph 121 above, the secrecy of the surveillance is achieved through arrangements calculated to conceal that the target's otherwise overt interlocutor is in effect an operative using or manipulating his or her position or relationships to obtain information for use by the authorities. The degree of intrusion resulting from the use of this surveillance technique is not necessarily any lesser in a given case than that entailed by the interception of communications – in particular since such operatives can likewise obtain access to the content of the target's communications. According to the Court's case-law, the decisive factor for assessing what level of safeguards is required in relation to a given surveillance technique is the degree of intrusion with the rights under Article 8 of the Convention that it entails rather than its technical definition (see *R.E. v. the United Kingdom*, no. 62498/11, §§ 126-30, 27 October 2015, with reference to *Bykov v. Russia* [GC], no. 4378/02, § 78, 10 March 2009, and *Uzun v. Germany*, no. 35623/05, § 66, ECHR 2010). That said, the specific requirements flowing from those principles may need to be adjusted to account for the differences between the intrusion entailed by the use of an "agent on cover" and the degree of intrusion entailed by other covert surveillance techniques such as the interception of communications.

(β) With regard to the manner of examination of those safeguards

144. In cases such as the present one – in which the applicant complains in the abstract about a system that allows covert surveillance rather than of specific instances of such surveillance – the relevant domestic laws must be scrutinised as they stand when the Court examines the application rather than as they stood when it was lodged (see *Centrum för rättvisa*, § 151, and

Big Brother Watch and Others, § 270, both cited above). The other point of relevance to this case is that the assessment of whether the laws in issue offer effective safeguards against abuse must be based not only on those laws as they are on paper, but also on (a) the actual operation of the surveillance regime in issue, and (b) the existence or absence of evidence that it has been abused (see *Centrum för rättvisa*, § 274, and *Big Brother Watch and Others*, § 360, both cited above).

(ii) Application of those principles

(α) Accessibility of the law

145. The 2008 regulations on "agents on cover" and their September 2018 amendments have both been officially published and are therefore accessible (see paragraphs 6 and 26 above).

(β) Grounds on which "agents on cover" may be used and persons who can be placed under surveillance by such agents

146. The relevant issue in relation to the grounds on which covert surveillance may be resorted to and the persons who can be placed under such surveillance is whether the law authorising such surveillance defines clearly enough (a) the nature of the offences or other grounds that may give rise to surveillance and (b) the categories of persons who may be placed under surveillance (see *Ekimdzhiev and Others*, cited above, § 298).

147. By regulation 52(1), an "agent on cover" may be deployed if there is a "proven operational need", and regulation 52(2) specifies that such a need exists if the Agency's statutory tasks cannot be discharged in another way (see paragraph 11 above). Read in conjunction with the statutory provisions defining the main tasks of the Agency – namely, to safeguard national security and carry out counterintelligence activities (see paragraph 42 above) – this means that "agents on cover" may only be deployed whenever necessary to attain those tasks. A simple reference to "national security" as the purpose for deploying such agents does not necessarily contravene Article 8 of the Convention; rather, what matters is whether any potential arbitrariness or abuse flowing from the inherently vague and indeterminate meaning and contours of the notion of "national security" can be checked (see *Ekimdzhiev and Others*, cited above, § 301). In the absence of (a) any effective independent scrutiny of the Agency's decision to deploy an "agent on cover" (the Court will revert to that matter in more detail in paragraphs 151-152, 156-159 and 163-164 below), and of (b) a requirement to provide clear and concrete reasons demonstrating the need to deploy such an agent in a specific case, a serious issue arises in this respect (contrast *Ekimdzhiev and Others*, cited above, § 301 *in fine*). It must further be noted in that connection that the tasks of the Agency, as set out in a number of statutes, extend across a wide range of domains – several of which do not

inherently concern unlawful conduct by potential targets (see paragraph 43 above). That significantly broadens the potential scope for deploying "agents on cover", and correspondingly increases the risk of arbitrariness or abuse.

148. By regulation 50, as amended in September 2018, "agents on cover" may be infiltrated (a) into the State administration, into legal persons and into civil associations, and (b) as persons exercising a "liberal profession" (except as lawyers in private practice); moreover, the wording of regulation 51 (as amended in September 2018) makes it plain that the position into which the "agent on cover" may be infiltrated need not necessarily be a position in a public entity (see paragraphs 28-29 above). From this, it can be inferred that theoretically any individual or private organisation in Bulgaria could find him-, her- or itself under surveillance by such agents, a situation which constitutes a significant interference into individual privacy rights, including a possible chilling effect on civic participation. The same considerations apply here: it is not the breadth of the potential field of work of such agents that is problematic in itself, but rather the absence of any effective independent check on potential arbitrariness or abuse.

(γ) Duration of the deployment of "agents on cover"

149. The regulations in issue do not subject the deployment of an "agent on cover" to any time-limits. Such agents can thus, theoretically, be deployed for indefinite periods – for as long as the Agency remains of the view that there is a "proven operative need" for their use. This is in marked contrast with the use of "special means of surveillance", the use of which is subject to time-limits – even when they are employed for national security purposes (see *Ekimdzhiev and Others*, cited above, § 305).

(δ) Deployment procedure

150. The relevant factors falling under this rubric are (a) the status of the authority that can authorise covert surveillance, and, if applicable, (b) the way in which that authority reviews surveillance requests and authorises surveillance (see *Ekimdzhiev and Others*, cited above, § 306).

151. A reading of regulations 52(3) and 53(2) (see paragraphs 11 *in fine* and 12 above) suggests that the procedure for deploying an "agent on cover" starts with a proposal made by the head of the respective division or unit of the Agency that wishes to deploy such an agent. That proposal – which must justify the existence of a "proven operational need" to use such an agent – is put to the head of the Agency, who decides whether to deploy the agent, and sets his or her specific tasks. The regulations make no provision for the approval of that deployment by any sort of independent outsider or at least for its notification to such an outsider (compare, *mutatis mutandis*, *Pietrzak and Bychawska-Siniarska and Others*, cited above, § 274).

152. It is true that, as already noted, by regulation 52(1), an "agent on cover" may be deployed if there is a "proven operational need", and that regulation 52(2) specifies that such a need exists if the Agency's statutory tasks cannot be discharged in another way (see paragraph 11 above). The manner in which those regulations are formulated thus introduces a degree of proportionality in the deployment of "agents on cover". However, the regulations give no indication of the factors that the head of the Agency must consider when assessing those points. In particular, the regulations do not require the head of the Agency to take his or her decision with reference to considerations relating to the Article 8 rights of the persons who stand to be affected by the agent's deployment, or to have regard to the degree to which the tasks assigned to the agent may intrude on the Article 8 rights of the target or of other persons (who might be collaterally affected by the agent's work), in particular where the agent's deployment is liable to give access to medical, journalistic, or legally privileged material or communications, which enjoy heightened protection under Article 8, or otherwise to situations in which the persons concerned may reasonably expect an enhanced degree of confidentiality. Nor do the regulations require the head of the Agency to carry out a proper balancing exercise in that regard. There is therefore no guarantee that "agents on cover" would be deployed only when genuinely necessary and proportionate in each case (see, *mutatis mutandis*, *Ekimdzhiev and Others*, cited above, § 321).

153. There is, moreover, no explicit requirement for the assessment of any such matters to be properly recorded by the Agency, so as to make it possible for the deployment of an "agent in cover" to be effectively scrutinised later.

(ε) Procedures for storing, accessing, examining, using, communicating and destroying data obtained as a result of the use of "agents on cover"

154. The regulations in issue state nothing about the storing, accessing, examining, using, communicating and destruction of data obtained as a result of the use of "agents on cover". It therefore seems that all those matters are governed by the general rules regulating how the Agency processes its operational data (see paragraphs 51-54 above). In the absence of any submissions by the parties on this point (see paragraphs 136-139 above), the Court is not prepared to delve further into this aspect of the case. It would simply note that, by contrast, relatively detailed provisions govern all those matters in relation to data obtained by using "special means of surveillance" – and that, still, various lacunae in those provisions led it to conclude that it was possible for such data to be misused for ends that have little to do with the statutory purpose for which they are collected (see *Ekimdzhiev and Others*, cited above, §§ 325-32).

(στ) Supervision

155. The factors relevant for deciding whether the supervision is adequate are (a) the independence of the supervisory authorities, their competences, and their powers (to access surveillance material and to redress breaches – in particular by ordering the destruction of surveillance material), and (b) the possibilities for effective public scrutiny of those authorities' work (see *Ekimdzhiev and Others*, cited above, § 334).

156. The regulations themselves make no provision for any supervision of the deployment or work of "agents on cover" (compare, *mutatis mutandis*, *Antunes Rocha v. Portugal*, no. 64330/01, § 77, 31 May 2005); moreover, as noted in paragraph 124 above, such agents fall outside the purview of the National Bureau for the Oversight of Special Means of Surveillance.

157. The special parliamentary committee tasked with supervising the Agency's work – the same as that which was in issue in *Ekimdzhiev and Others* (cited above, § 125) – although capable of dealing with individual cases, cannot order remedial measures; if it spots irregularities, it can only bring them to the attention of the prosecuting or other competent authorities (see paragraph 55 above). Moreover, that committee's members are not required to have any legal qualifications or experience (see *Ekimdzhiev and Others*, cited above, § 414). Nor does it seem that the committee has in practice exercised detailed and regular control over the Agency's operations in general – let alone control specifically focusing on its use of "agents on cover" – or has ever got involved in the Agency's day-to-day work (compare *Ekimdzhiev and Others*, cited above, § 345, and, *mutatis mutandis*, *Szabó and Vissy v. Hungary*, no. 37138/14, § 82, 12 January 2016; also contrast *Leander*, cited above, §§ 40 and 65).

158. There is no indication that the Agency's head, deputy heads or officers have ever been called to the Bulgarian Parliament to report on the use by the Agency of "agents on cover" (see paragraph 56 above). Nor is there any indication that the point has been adverted to in reports by the Agency to the Government or the President of the Republic (see paragraphs 57-58 above). In any event, such general political control can hardly be considered independent (see, *mutatis mutandis*, *Association for European Integration and Human Rights and Ekimdzhiev*, § 87, and *Szabó and Vissy*, § 75, both cited above), or sufficient to prevent individual abuses.

159. Nor does it seem that the Agency's operations involving the use of "agents on cover" have ever been checked by the Commission for Protection of Personal Data – which under section 37 of the 2007 Act supervises the processing of personal data by the Agency (see paragraph 72 above). Indeed, as noted in paragraph 128 above, it is unclear whether the power that section 37 bestows upon that Commission relates to operational data gathered by the Agency.

160. In view of the above considerations, the system for supervising the use of "agents on cover" does not appear capable of providing effective

guarantees against their arbitrary or abusive deployment by the Agency (see, *mutatis mutandis*, *Ekimdzhiev and Others*, cited above, § 347), or against the risk of misuse of power by the "agents on cover" themselves – which, as the practice of other States shows, can be seen as real in the absence of proper supervision (see the comparative-law information referred to in *Veselov and Others v. Russia*, nos. 23200/10 and 2 others, §§ 50 and 62, 2 October 2012).

(ζ) Notification

161. The relevant factors under this rubric are (a) whether it is possible for the authorities to notify a target person or entity that an "agent on cover" has been deployed against him, her or it, and (b) whether such notification constitutes a prerequisite for resorting to any available remedies (see *Ekimdzhiev and Others*, cited above, § 348).

162. The regulations in issue, as amended in September 2018, make no provision for anyone to be notified – under any circumstances and at any point – of the use of an "agent on cover". Neither can any such notification be made by the National Bureau for the Oversight of Special Means of Surveillance (see paragraph 124 above). It does not appear that there is provision for such notification elsewhere in Bulgarian law. Nor does it seem possible for persons possibly affected by the use of such agents to obtain information about such use under the provisions governing access to personal data processed by the Agency (see paragraphs 125-127 above), or under the general data protection legislation (see paragraph 128 above). This absence of notification or information, although not necessarily problematic in itself (since the disclosure of the fact that an "agent on cover" has been deployed in a particular organisation would in many cases inevitably give clues about the identity of that agent, or even be effectively tantamount to disclosing his or her identity), in turn affects the possibilities for those persons to seek a remedy (see paragraphs 133-134 above).

(η) Remedies

163. As noted in paragraph 124 above, the special remedy put in place in 2009 with respect to "special means of surveillance" – a claim for damages for their unlawful use (see *Ekimdzhiev and Others*, cited above, §§ 136-44 and 265-72) – does not apply to "agents on cover". The data protection remedy under section 36(4) and (9) of the 2007 Act does not appear to be effective in relation to them either. The same goes for the possibilities of (a) complaining to the Commission for Protection of Personal Data, (b) resorting to the other general data protection remedies under the 2002 Act, (c) seeking judicial review of the decisions of the head of the Agency, and (d) engaging the personal liability of "agents on cover" (see paragraphs 125-134 above).

164. It follows that Bulgarian law does not provide an effective remedy with respect to the use of "agents on cover".

(θ) Conclusion

165. In sum, the regulations governing the use of "agents on cover" fall short of the minimum safeguards against arbitrariness and abuse required under Article 8 of the Convention in the following respects:

(a) the broadly-defined grounds on which such agents can be deployed and fields in which they can be deployed, coupled with the way in which that deployment is decided, are capable of leading to arbitrariness and abuse (see paragraph 146-148 above);

(b) no time-limits circumscribe the use of such agents (see paragraph 149 above);

(c) the procedure for deploying such agents does not appear capable of ensuring that they will be used only when "necessary in a democratic society" (see paragraph 151-153 above);

(d) no arrangements exist for effective supervision of the use of such agents, which can lead to arbitrariness and abuse, as well as to corruption or the misuse of power by the "agents on cover" themselves (see paragraphs 156-160 above); and

(e) there is no remedy in relation to the unlawful or unjustified use of such agents (see paragraphs 163-164 above).

166. It is true that there is no evidence that those shortcomings in the legal regime have had an actual impact on the use of "agents on cover" in Bulgaria. But since that use is by definition clandestine and no information is available about it in the public domain, no decisive weight can be attached to that lack of evidence of arbitrariness or abuse. Moreover, the regulations were amended relatively recently (in September 2018) to make it possible for "agents on cover" to be infiltrated into private organisations and "liberal professions".

167. It follows that the Bulgarian domestic provisions on "agents on cover" do not meet the quality-of-law requirement and are incapable of keeping the interference with rights protected under Article 8 of the Convention entailed by the use of such agents to what is "necessary in a democratic society".

168. There has therefore been a breach of Article 8 of the Convention.

II. APPLICATION OF ARTICLE 41 OF THE CONVENTION

169. Article 41 of the Convention provides:

> "If the Court finds that there has been a violation of the Convention or the Protocols thereto, and if the internal law of the High Contracting Party concerned allows only partial reparation to be made, the Court shall, if necessary, afford just satisfaction to the injured party."

A. Damage

1. The association's claim and the Government's comments on it

170. The applicant association claimed 4,000 euros (EUR) in respect of the non-pecuniary damage that it had allegedly suffered as a result of the impugned regulations.

171. The Government contested the claim in full, noting that in similar previous cases no award had been made in respect of non-pecuniary damage. In the alternative, they submitted that the claim was exorbitant, since there was no evidence that those regulations had resulted in any actual interference with the association's rights under Article 8 of the Convention.

2. The Court's assessment

172. As attested by the adjective "just" and the phrase "if necessary" in Article 41 of the Convention, the Court enjoys discretion in the exercise of the power to afford such satisfaction to the injured party (see, as a recent authority, *Molla Sali v. Greece* (just satisfaction) [GC], no. 20452/14, § 32, 18 June 2020). In some cases, the public vindication of the wrong suffered by that party, in a judgment binding on the respondent State, can in itself amount to sufficient redress. This is especially so when, as here, (a) the finding of breach is based solely on the conclusion that a law, procedure or practice has fallen short of Convention standards (ibid., § 33, with reference to *Varnava and Others v. Turkey* [GC], nos. 16064/90 and 8 others, § 224, ECHR 2009), without a further finding that this shortcoming has affected the applicant in any tangible way, and (b) general measures would constitute the most appropriate form of redress (see paragraph 4 of the Practice Direction on Just Satisfaction Claims, as amended in June 2022).

173. In the present case, no evidence has been produced to show that the existence of the regulations on "agents on cover", as amended in September 2018, has caused the applicant association any tangible detriment. The association did not even specify the nature of the non-pecuniary damage that it had allegedly suffered on that account. Even if it is accepted that it has indeed suffered some damage of that sort on account of the mere existence of those regulations, the finding of a breach of Article 8 of the Convention affords it sufficient just satisfaction in that regard (see *Ekimdzhiev and Others*, cited above, § 426, with further references). It is, then, not necessary to award it any monetary compensation in respect of such damage.

174. It must at the same time be emphasised that under Article 46 of the Convention, a judgment in which the Court finds a violation of the Convention or its Protocols imposes on the respondent State an obligation to choose, subject to supervision by the Committee of Ministers, the general and/or, if appropriate, individual measures to be taken in its domestic legal order to end the violation and make all feasible reparation for its

consequences in a way to restore as far as possible the situation which would have obtained if the violation had not taken place. Moreover, it follows from the Convention, and from its Article 1 in particular, that in ratifying it the Contracting States undertook to ensure that their domestic laws would be compatible with it (see *Ekimdzhiev and Others*, cited above, § 427).

B. Costs and expenses

175. The applicant association sought reimbursement of EUR 3,500 said to have been incurred during the proceedings for judicial review of the impugned regulations, and EUR 3,000 said to have been incurred for the services of the lawyer who had represented it before the Court. It produced no documents in support of those claims.

176. The Government pointed out that the claims were neither itemised nor supported by evidence, and invited the Court to dismiss them. In the alternative, they argued that the claim relating to the proceedings before the Court was exorbitant, since the volume of the submissions made on behalf of the association and of the case file did not warrant such a high level of costs.

177. According to the Court's case-law, applicants are entitled to the reimbursement of costs and expenses only in so far as it has been shown that these were actually and necessarily incurred and are reasonable as to quantum. Since the association produced no documents in support of its claim, there is no basis on which to find that it actually incurred the costs and expenses whose reimbursement it seeks (see also paragraphs 18 and 21 of the Practice Direction on Just Satisfaction Claims, as amended in June 2022). In those circumstances, and bearing in mind also the terms of Rule 60 §§ 2 and 3 of the Rules of Court, the Court makes no award under this head.

FOR THESE REASONS, THE COURT, UNANIMOUSLY,

1. *Joins* the Government's objections that the applicant association has not exhausted the available domestic remedies and that it cannot claim to be a victim of interference with its rights under Article 8 of the Convention to the merits, and *dismisses* them;

2. *Declares* the application admissible;

3. *Holds* that there has been a violation of Article 8 of the Convention;

4. *Holds* that the finding of a violation of Article 8 of the Convention amounts to sufficient just satisfaction in respect of any non-pecuniary damage suffered by the applicant association;

5. *Dismisses* the remainder of the applicant association's claim for just satisfaction.

Done in English, and notified in writing on 17 February 2026, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

Milan Blaško Registrar	Ioannis Ktistakis President