Complaint under Article 34 of the ECHR

A. Facts

I. Overview

1 The applicant seeks to defend itself against the German Act on Restrictions on the Secrecy of Mail, Post and Telecommunications (*Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses*, also known as the G10 Act or G10) as interpreted by the German Federal Administrative Court (*Bundesverwaltungsgericht - BVerwG*) and the German Federal Constitutional Court (*Bundesverfassungsgericht - BVerfG*). The G10 Act grants the German Foreign Intelligence Agency (*Bundesnachrichtendienst* - hereinafter referred to as the BND) the authority to secretly conduct large-scale surveillance of telecommunications traffic using search terms and to examine all communications that produce 'hits' as regards "relevance for intelligence purposes" (*"nachrichtendienstliche Relevanz"*).

2 Notwithstanding that the BND secretly monitors many millions of communications in this way year after year, there is no effective judicial remedy against this surveillance. Only in a few exceptional cases does the law provide for the notification of those affected. Whether such notification ever actually takes place is not known. What is known is that in the last 40 years there has not been a single case in Germany in which the BND's measures have been subjected to examination by a court on account of such notification.

3 Without such notification those affected by the monitoring are unable to assert their right to recourse to the courts because the Federal Administrative Court and the Federal Constitutional Court require that complainants furnish full proof of their being directly affected. However, if the BND does not notify the complainants that they were subject to the surveillance measures the latter have no means of providing such proof due to the secret nature of the measures and the complete deletion of all recorded communications, with the result that to all intents and purposes access to an effective remedy is completely lacking.

4 In addition to the lack of effective judicial remedy, the surveillance itself clearly breaches the Convention in that it is grossly disproportionate. The BND screens hundreds of millions of communications every year. In 2013 alone, this

generated 15,401 "hits" that were read manually, with less than 120 of those communications being identified as relevant for intelligence purposes.

5 The provisions of the G10 Act regulating "strategic telecommunications surveillance" (*"Strategische Fernmeldeüberwachung"*) have their origins in the first G10 Act that dates back to 1968 and which was the subject of the judgment of the European Court of Human Rights (ECtHR") of 6.9.1978 (ECtHR Judgement of 6.9.1978, Application No 5029/71 - Klass and Others v. Germany).

6 In the judgment of 6.9.1978 the ECtHR took the view that the version of the G10 Act that applied at that time guaranteed access to a legal remedy that satisfied the requirements set out in Article 13 of the ECHR. In its judgment, the ECtHR assumed that affected parties would as a rule be notified of such monitoring (Loc. cit, margin number 71):

> *"From the moment of such notification, various legal remedies - before the courts - become available to the individual. According to the information supplied by the Government, the individual may: in an action for a declaration, have reviewed by an administrative court the lawfulness of the application to him of the G 10 and the conformity with the law of the surveillance measures ordered; bring an action for damages in a civil court if he has been prejudiced; bring an action for the destruction or, if appropriate, restitution of documents; finally, if none of these remedies is successful, apply to the Federal Constitutional Court for a ruling as to whether there has been a breach of the Basic Law (see paragraph 24 above)."*

7 As set out in the following, there has been a dramatic increase in the scope of the G10 measures (which at the time only affected telephone conversations) since 1978. At the same time, the G10 Act was formulated such that in practice affected parties are either not notified at all or only in extremely rare cases. Owing to the lack of such notification, these surveillance measures have never been subject to a court revision – contrary to the expectations expressed by the ECtHR in the Klass judgement.

8 The combination of far-reaching, unfounded surveillance powers for the BND pursuant to the G10 Act and the de facto lack of legal remedy through the courts for those affected violates the applicant's right to respect for private and family

life (Article 8 of the ECHR), its right to freedom of expression (Article 10 of the ECHR) and its right to effective remedy (Article 13 of the ECHR).

II. Legal grounds

1. Statutory authorisation

9 The"strategic telecommunications surveillance" is regulated by the G10 Act in its version of 26 June 2001 **(Annex 2, pp. 21-32).** The G10 Act (in its earlier versions) had already been the subject of rulings by the Court (in addition to the ECtHR judgment of 6.9.1978, Application No 5029/71 - Klass and Others v. Germany (see margin number 5) also the ECtHR judgment of 29.6.2006, Application No 54934/00,– Weber and Saravia v. Germany.).

10 Pursuant to **Section 5 (1) in conjunction with Section 10 (1) of the G10 Act,** the BND can apply to have the Federal Ministry of the Interior order restrictions (= surveillance measures) on international telecommunications contacts. The term "telecommunications contacts" ("Telekommunikationsbeziehungen") within the meaning used here refers to all forms of telecommunication, in particular also email traffic. In this context, copies are secretly made of all monitored telecommunications, e.g. emails, then sent to the BND and screened by the latter for search terms.

11 **Section 10 (4) of the G10 Act** stipulates that in cases of strategic telecommunications surveillance the search terms must be specified in the order establishing the surveillance. Furthermore, the area across which data is to be gathered and the transmission paths to be subject to the restriction of privacy must also be specified. In addition, the percentage of available transmission capacity of the transmission paths that is to be subject to surveillance must be defined. In cases in which Section 5 of the G10 Act applies, that percentage may not exceed 20 percent.

2. Affected parties generally not notified

12 Under Section 12 (1) of the G10 Act, those affected by measures restricting privacy are to be informed of the measures after they have ended. However, Section 12 (1) of the G10 Act provides for numerous exemptions from the obligation to notify affected parties. The most far-reaching exemption arises from **Section 12 (2) of the G10 Act,** according to which the obligation to notify

the affected party no longer applies if communications that have been read are "deleted immediately".

13 Pursuant to **Section 6 (1) of the G10 Act** any communication that is classified as irrelevant for intelligence purposes is to be deleted. The same applies for communications that are not found to contain pertinent search terms in the screening process. As a result – if at all – only those persons receive notification whose communications are classified as relevant. In 2013 that was 118 emails out of presumably hundreds of millions of monitored communications.

14 All deletions are recorded in a protocol pursuant to **Section 6 (1) sentence 3 of the G10 Act,** whereby the protocol data is to be deleted at the end of the calendar year following the year in which the protocol was made (Section 6 (1) sentence 5 of the G10 Act). Except in cases in which communications are deemed to be of relevance for intelligence purposes, **1 year after the monitoring period ends all individual data** regarding the surveillance measures is no longer available.

15 Consequently, practically all those affected only learn that their email traffic may have been monitored in the context of "strategic telecommunications surveillance" from the annual report compiled by the German Bundestag's Parliamentary Control Panel (*Parlamentarisches Kontrollgremium – PKGr*). Pursuant to Section 14 (1) of the G10 Act, the Parliamentary Control Panel is to be informed at intervals of no longer than six months according to the provisions set out in Section 1 et seq. of the Act on Parliamentary Control of Intelligence Activities (*Kontrollgremiumgesetz – PKGrG*) **(Annex 3, pp. 33-36)** about the performance of G10 surveillance measures. The Parliamentary Control Panel, for its part, "*submits to the German Bundestag an annual report on the execution as well as the nature and scope of measures that fall under Sections 3, 5, 7a and 8, …* (Section 14 (1) sentence 2 of the G10 Act). The report is limited to a few abstract comments.

3. Paliamentary supervision

16 In addition to the activities of the Parliamentary Control Panel, the BND's measures in the context of "strategic telecommunications surveillance" are also examined **by the so-called "G10 Commission" pursuant to Section 15 of the G10 Act**. The Federal Ministry of the Interior informs the G10 Commission on a

monthly basis about any measures it orders restricting privacy – as a rule before the execution of such measures (**Section 15 (6) of the G10 Act**). The G10 Commission decides *ex officio* or on account of complaints on the permissibility or necessity of monitoring measures. **(Section 15 (5) of the G10 Act**). Any orders for monitoring which the commission declares impermissible or unnecessary are to be cancelled immediately by the responsible federal ministry **(Section 15 (6) sentence 6 of the G10 Act)**.

17 The G10 Act explicitly names two constellations in which such measures are reviewed by the Parliamentary Control Panel and the G10 Commission instead of through a legal process (Section 13 of the G10 Act). This is the case for monitoring of individuals (Section 3 of the G10 Act) and in cases of strategic restrictions owing to the threat of armed aggression against the Federal Republic of Germany (Section 5 (1) sentence 3 No 1 of the G10 Act).

18 If neither of these two constellations applies, in the context of strategic surveillance only a theoretical possibility exists to lodge an abstact, general complaint. The G10 Commission does not have the powers of a court in such matters.

19 The deputy chair of the G10 Commission, Bertold Huber, has however stated regarding the frequency of the Commission's supervisory activities that the Commission has never had to rule on a complaint lodged by a party affected under Section 5 of the G10 Act. In the years 2012 and 2011, not a single complaint was lodged on account of surveillance measures performed pursuant to Section 5 of the G10 Act.

Proof: Answer sheet of the G10 Commission of 9.5.2014 **(Annex 6, pp. 98-104**), alternatively: hearing of Dr. Bertold Huber, to be summoned to testify as a witness via the G10 Commission at the German Bundestag, Platz der Republik 1, 11011 Berlin.

III. Factual basis

1. The BND's methods

20 As already explained above, Section 5 (2) of the G10 Act confers upon the BND the authority to screen emails and other "telecommunications traffic" using search terms. A distinction is made between "formal" search terms and

"content" search terms. Whereas formal search terms refer to data that can be assigned to a specific foreign target person (e.g. email addresses, names, etc.), content search terms are general terms in everyday usage. The use of content search terms in particular leads to emails being examined by the BND arbitrarily and without any grounds (for instance because a certain term was used in the communication) (see below).

21 The general conditions for monitoring set out in the Act do not in effect impose any restrictions on the surveillance. Although **Section 10 (4) sentence 2 of the G10** stipulates that the BND must **specify** in its applications **"the area"** to be tracked through the surveillance, in the risk area "international terrorism" the "area" subject to BND surveillance in 2010 covered practically the **entire globe**. 150 states and 46 other regions were affected by the BND's surveillance measures. The surveillance covered communications with almost every country in Europe as well as with the United States.

Proof: Annual main application by the BND for the INTT Area in 2010 (including a list of all telecommunications contacts) **(Annex 5, pp. 46-97, in particular pp. 92-97)**

22 Furthermore, in cases of surveillance pursuant to Section 5 of the G10 Act, the **percentage** of the **available transmission capacity of the transmission paths subject to surveillance must not exceed 20 percent** (Section 10 (4), sentence 4 of the G10 Act). This requirement also does not de facto restrict the surveillance in any way given that the transmission capacity of the path is generally **many times higher than the actual transmission volume**. Indeed, it is even likely that the BND can gain access to **all the email traffic** passing through a given transmission path. In any case, telecommunications users should assume that this is the case.

23 For example, Germany's largest internet exchange point, the DE-CIX data carrier based in Frankfurt, has a transmission capacity of 22.6 tbit/s. Statistics put out by DE-CIX show that the maximum daily average throughput over a year for its networks is just 5.9 tbit/s, however, on average they work at a capacity of only 3.4 tbit/s. That means that just 20 percent or less of the total transmission

capacity is used. Reports show that the BND accesses the DE-CIX Internet exchange points.

Proof:

1. DE-CIX press release of 11.5.2017 **(Annex 14, pp. 235-238)**
2. DE-CIX statistics, called up on 27.11.2017 **(Annex 16, pp. 240-244)**
3. SPIEGEL ONLINE report of 16.9.2016 **(Annex 9, pp. 159-162)**
4. DIE ZEIT report of 16.9.2016 **(Annex 10, pp. 163-165)**
5. Statement by Prof. Dr. Matthias Bäcker on the hearing in the NSA investigating committee on 22.5.2014 **(Annex 7, pp. 105-128)**

24 On the basis of an order pursuant to Section 12 (4) of the G10 Act, the BND instructs telecommunications companies (such as Deutsche Telekom AG) that operate internet exchange points in Germany to "duplicate" the entire data traffic passing through designated routes and to pass on the "duplicate" to the BND — without the communication parners being aware of this.

25 In a first step the BND then attempts to filter out all emails sent within Germany, to which, as a foreign intelligence service, it should not under any circumstances have access. Once this filtering process is completed, the remaining emails are screened for search terms. All emails identified using the search terms (the "hits") are read ("processed for intelligence") by BND staff in order to determine whether the emails are "relevant for intelligence purposes". Communications that are deemed "irrelevant" are deleted (Section 6 (1) of the G10 Act). In such cases, the persons concerned are not notified (see margin number 12 et seq.).

26 Persons whose emails have been monitored or read first learn about the surveillance measures when the Parliamentary Control Panel publishes its annual report (see margin number 15). This report is generally published more than a year after the conclusion of the report period and therefore only after all individual data about the BND's activity has been deleted without a trace (see margin number 15).

Proof: List of the times of publication **(Annex 17, p. 245).**

2. The applicant and the surveillance measures in 2013

27 The applicant is a registered association based in Berlin **(Annex 18, p. 246)**. Its declared mission is to document violations of press freedom and freedom of information worldwide and to alert the public when journalists or the people who work with them are in danger. It campaigns against censorship and restrictive media laws. The applicant is part of the international organisation "Reporters sans frontières", founded in 1985 and based in Paris. The German section is, however, independent both financially and in terms of its organisation. Owing in particular to the international character of the applicant's activities, the applicant has for many years now communicated frequently with foreign members of the organisation, a large number of journalists and other conversation partners, for the most part via email.

28 A geographical focus of the applicant's activities is the Middle East (including Egypt, Syria, Bahrain, Saudi Arabia, Lybia) as well as almost all the states of the former USSR (including Russia, Uzbekistan, Kazachstan, Belarus, Azerbaijan, etc.) According to media reports, many BND operations target these regions of the world. Precisely the strong commitment of the applicant to providing emergency aid to journalists on site and in exile indicates an increased threat of surveillance, since in the context of this work information on visa procedures, help for the families of journalists under threat, bail money, border crossings and similar issues is frequently discussed with affected journalists. Specific cases of surveillance of journalists have already been established in the past. The NDR journalist Stefan Buchen was targeted for monitoring by the BND and CIA because he was in frequent contact with persons in those regions. In 2013 the applicant also conducted intense research in the area of illegal exports of surveillance technology to authoritarian states such as Bahrain, Libya, Egypt and Russia, and on the question of how these exports can be regulated in the context of arms exports controls. For this purpose, an intense exchange of emails takes place between the applicant and civil society organisations and technical experts worldwide.

29 The applicant sent and received approximately **280,000 international emails** in 2013. As an association founded by journalists to campaign for journalists, the

applicant's emails deal with many different matters. The applicant would like to stress here that in recent times it has dealt in particular with the activities of intelligence services across the globe and in Germany.

30 **The annual report of the Parliamentary Control Panel of the German Bundestag (PKGr) of 08.01.2015** shows that the **BND** carried out measures for the surveillance of international telecommunications traffic on a large scale **in 2013**. In the course of its telecommunications traffic surveillance the BND identified the high figure of **15,401 "hits"**, which were then processed for intelligence purposes, or in other words read.

31 The total number of emails monitored by the BND in 2013 is not known. What is clear is that it must have been considerably more than 15,041 emails, because that figure refers merely to the "hits". Based on the hypothesis that there was one hit for every 1,000 emails, one would conclude that the **total volume of emails monitored was 15 million**. The real figure is likely to be far higher, as the hit statistics (and the implicit scope of the surveillance) from the preceding years indicate.

Proof: Proof: Parliamentary Control Panel report for 2013 of 08.01.2015 **(Annex 4, pp. 37-45)**

32 According to the Parliamentary Control Panel report, the BND achieved this high number of hits using thousands of search terms. In the risk area "international terrorism" **792 search terms** were used, in the risk area "proliferation of weapons of war and trade in conventional arms" **11,704 search terms** were used, and in the area "illegal smuggling" **27 search terms** were used. Which precise terms were used is not known. However, the BND did admit that the search terms used include "common terms related to current events". Press reports according to which search terms such as "bomb" were used seem plausible.

Proof: Proof: Parliamentary Control Panel report of 08.01.2015 for 2013 **(Annex 4, pp. 37-45, in particular p. 44)**

33 In other words, the BND used 12,523 search terms in 2013 to screen hundreds of millions of emails, then classified more than 15,000 of them as suspicious and subjected them to an evaluation (= processing by an employee of the BND). Of

the 15,401 "hits" only 118 were classified as "relevant for intelligence purposes". What precisely is to be understood by "relevance for intelligence purposes" (*"nachrichtendienstliche Relevanz"*) is not known.

34 It is highly likely that correspondence sent or received by the applicant was among the "hits". It is almost certain that emails of the applicant were among the millions of mails that were scanned for search terms but did not generate a hit.

35 By the start of 2015, when the applicant first learned from the Parliamentary Control Panel's report for 2013 that the BND had monitored emails on a large scale, only the 118 "telecommunications" from 2013 that the BND had "classified as relevant for intelligence purposes" were still stored at the BND.

IV. Prior proceedings and court decisions

36 The applicant appealed to the German courts to rule that in 2013 in the course of its strategic telecommunications surveillance pursuant to Section 5 (1) of the G10 Act the BND had violated the secrecy of telecommunications under Article 10 of the Basic Law (*Grundgesetz - GG*). On 30.6.2015 the applicant filed a suit with the Federal Administrative Court (BVerwG) aimed at establishing the illegality of the strategic telecommunications surveillance measures.

Proof: Applicant's complaint of 30.6.2015 **(Annex 8, pp. 129-158)**

37 In its decision of 14.12.2016, served on the applicant on 27.1.2017, the Federal Administrative Court dismissed the lawsuit as inadmissible. The Court found a lack of determinable interest (*"festellungsfähige Interesse"*) within the meaning of Section 43 (1) of the Code of Administrative Court Procedure (*Verwaltungsgerichtsordnung - VwGO*), since a violation of the applicant's right to confidentiality of telecommunications pursuant to Article 10 of the Basic Law was no longer ascertainable and proof of the applicant's having been subject to monitoring was therefore lacking. It found that among the 118 telecommunications that were classified as “relevant for intelligence purposes” and were still accessible at the BND at the time there was no email correspondence sent or received by the applicant.

Proof: Judgment of the Federal Administrative Court of 14.12.2016, BVerwG 6 A 2.15 **(Annex 11, pp. 166-181)**

38 In its decision the Federal Administrative Court considered that it "could not be ruled out" that correspondence belonging to the applicant was among the hundreds of millions of emails monitored by the BND in 2013 and was screened for search terms, but either didn't produce any hits or was deleted by BND staff because it was considered "irrelevant for intelligence purposes" (Judgement of the Federal Administrative Court of 14.12.2016, BVerwG 6 A 2.15, **annex 11, pp. 166-181** (margin number 16). However, as it was no longer possible to "ascertain" whether correspondence belonging to the applicant was among the communications that were recorded and examined, it could not be ruled that a "determinable legal relationship" within the meaning of Section 43 (1) of the Code of Administrative Court Procedure (VwGO) existed.

39 According to the judgement of the Federal Administrative Court, a lawsuit is admissible only if the applicant can prove that their correspondence was screened by the intelligence agency. It is, however, de facto impossible to furnish such proof without an explicit notification from the BND regarding the carrying out of the surveillance measure.

40 On 27.2.2017 the applicant lodged a constitutional complaint against the decision of the Federal Administrative Court with the Federal Constitutional Court. The applicant complained that the form of strategic telecommunications surveillance practiced by the BND violated the applicant's rights under Article 19, paragraph 4 (the guarantee of recourse to the courts), Article 10 (the right to privacy of telecommunications), Article 12 (occupational freedom) in conjunction with press freedom (Article 5 of the Basic Law) and Article 3 (principle of equality before the law) of the Basic Law. The Federal Constitutional Court dismissed the applicant's complaint in its decision of 26.4.2017 as inadmissible on the grounds that the applicant had not substantiated the claim of being affected. The applicant was notified of the decision in a letter dated 30.5.2017, which it received on 31.5.2017.

Proof: 1. Constitutional complaint by the applicant of 27.2.2017 **(Annex 12, pp. 182-233)**

2. Decision of the Federal Constitutional Court of 26.4.2017 (File no. 1 BvR 458/17) **(Annex 13, pp. 234-235)**

3. Letter by the Federal Constitutional Court of 30.5.2017 regarding the sending of the letter **(Annex, p. 239)**

B. Statements of violations

41 The decisions of the German courts violate the applicant's **right under Article 13 of the ECHR (see III. below)** In addition, the strategic telecommunications surveillance as carried out by the BND in 2013 violates the applicant's **right under Article 8 of the ECHR (see I. below) and under Article 10 of the ECHR (see II. Below)**.

I. Violation of Article 8, paragraph 1 of the ECHR

42 The right of the applicant under Article 8 of the ECHR was violated by the extensive and disproportionate surveillance measures of the BND in 2013.

1. Applicant's victim status

43 In accordance with Article 8, paragraph 1 of the ECHR, everyone has the right to respect for his private and family life, his home and his correspondence. According to the ECtHR's case law, the protection provided by Article 8, paragraph 1 of the ECHR covers telecommunications via email as well as telecommunications traffic data. (ECtHR Judgement of 3.4.2007, Application No 62617/00, § 41 – Copland v. United Kingdom). The confidentiality of all correspondence between persons is protected (ECtHR Judgement of 27.10.2015, Application No 62498/11). This protection applies regardless of the content of the communication (ECtHR Judgement of 6.12.2012, Application No 12323/11, § 90 – Michaud v. France), with the result that business correspondence is also covered by Article 8 of the ECHR.

44 The secret surveillance is an intense encroachment on the individual's right to respect for his private life and his correspondence. Moreover, as regards communication via emails and other Internet-based services, the very **existence of laws** providing for their surveillance already constitutes a threat to the freedom of communication, particularly since technogical advances have enabled "mass surveillance" and considerably intensify the encroachment on freedom of communication (ECtHR Judgement of 12.1.2016, Application No 37138/14, § 53 – Szabó and Vissy v. Hungary).

45 In the assessment of whether an applicant is affected, the question of whether the law in question affects a group of persons or **each user of communications services directly** plays a decisive role (ECHtR Judgement of 4.12.2015, Application No 47143/06, §§ 170-172 – Zakharov v. Russia). Section 5 (1) of the G10 Act stipulates that strategic telecommunications surveillance is not a measure against individuals but a general measure: the telecommunications traffic between Germany and abroad is systematically monitored using search terms. The identity of the sender and the recipient of an email plays no role (in contrast to cases involving measures against individuals). Owing to the use of thousands of search terms, whether a user uses one of these terms and the BND classifies this email as a hit and gains knowledge of its contents is a matter of pure chance. Consequently, **anyone** can be affected by this strategic telecommunications surveillance, without this being compensated for by effective recourse to legal remedy (see below margin number 61 et seq.)

46 According to the case law of the ECtHR, a party is considered affected if there is **a "reasonable likelihood"** that they were subject to monitoring (cf. ECtHR Judgement of 25.6.1997, Application No 20605/92 – Halford v. United Kingdom). The mere possibility of monitoring enhances the "chilling effects" and considerably restricts the freedom of telecommunications.

47 A reasonable likelihood of monitoring of the applicant's communications exists. The applicant **must assume** – given the lack of any meaningful restrictions on the surveillance (see above regarding "area", margin number 21; regarding capacity, margin number 22 et seq.; and the information regarding the search terms in general, margin number 32 et seq.) – that 1) its email communications were monitored by the BND, and that 2) owing to the use of inadequate filters they were subject to further processing.

48 Independently of this, owing to the **large scale of the surveillance** and **the applicant's intense exchange of emails** with foreign members of the organisation, many journalists and other communication partners it is almost certain that **emails sent by or to the applicant were among those that were screened for search terms by the BND**. The **high number of "hits"** alone leads to the conclusion that hundreds of millions of emails were screened by the BND using the search terms (see above).

49 In addition, the possibility **can certainly not be excluded** that an email sent or received by the applicant was **classified as a hit** in the search term screening procedure, but upon closer examination by BND staff pursuant to Section 6 (1) sentence 1 of the G10 Act turned out not to be “relevant for intelligence purposes”. Here too, owing to the activities of the applicant and the content of the emails it sent and received, there is a high probability that this was the case.

50 It is therefore of no consequence that the applicant cannot prove that it and its email correspondence were subject to the surveillance measures or that its emails were among the 15,401 hits or even the millions of emails that were affected by the secret measures of the BND in 2013.

2. No justification

51 The large-scale email surveillance is also not justified under Article 8, paragraph 2 of the ECHR. Although there is no doubt that the law provides for this monitoring, the BND's surveillance practices regarding emails violate the **prohibition of excessive measures** and are disproportionate.

a. The criterion of necessity

52 For determining whether a surveillance measure is necessary, the principle of proportionality, for which factors such as the nature, scope and duration of the monitoring are also to be considered, plays a key role (ECtHR Judgement of 6.9.1978, Application No 5029/71, § 50 – Klass and Others v. Germany). The exception provided for in Article 8, paragraph 2 of the ECHR must therefore be narrowly interpreted owing to the danger of abuse by the State (ECtHR Judgement of 12.1.2016, Application No 37138/14, § 54 – Szabó and Vissy v. Hungary).

53 In the light of technological advances and the possibility of mass surveillance, the ECtHR considers not just simple necessity but "strict necessity" to be a prerequisite for secret surveillance (ECtHR Judgement of 12.1.2016, Application No 37138/14, § 54 – Szabó and Vissy v. Hungary). In the view of the Court, for "strict necessity" to exist the secret surveillance must serve on the one hand to safeguard democtractic institutions and on the other hand to acquire "vital intelligence". Whether "strict necessity" exists is, furthermore, as a rule questionable if orders for surveillance are not subject to judicial supervision

(ECtHR Judgement of 12.1.2016, Application No 37138/14, § 75 – Szabó and Vissy v. Hungary).

b. Inadequate restrictions on the measures

54 Secret surveillance can serve to guarantee national security. However, the limits of proportionality must not be overstepped here. The greater the leeway granted for surveillance measures, the less significant freedom of communication becomes. If the individual has the feeling that he is being monitored, this provokes a diffuse sense of fear, the so-called **"chilling effect"**. Users of telecommunications services no longer feel free; they no longer regard their communications as private. They choose their words carefully in order to avoid being caught up in the intelligence agencies' "data hoover". With strategic telecommunications surveillance there is even the danger of the State obtaining information related not just to general circumstances, but also to private and even **intimate details in the communications of its citizens** as the contents of the emails are screened (first in an automated process and then by individual staff members). The consequence is self-censorship. The **dangers this entails for a free and democratic society** are obvious.

55 The German State does not just read a few emails in the course of surveillance; in 2013 it read more than 15,000 emails. As a result, the State gains access to far more information than it needs for fighting crime and terrorism. According to the the BND's own statements, only 118 of the emails "viewed" in this procedure were found to be "relevant". What exactly is to be understood by "relevant for intelligence purposes" is not at all clear.

56 In its concrete form determined by the provisions for strategic telecommunications surveillance set out in Section 5 of the G10 Act, the surveillance takes on entirely new scale. Whereas the cases ruled upon by the ECtHR *Klass and Others v. Gremany* (ECtHR Judgement of 6.9.1978, Application No 5029/71 - Klass and Others v. Germany) and *Weber and. Saravia v. Germany* (ECtHR Judgement of 29.6.2006, Application No 54934/00, § 78 – Weber and Saravia v. Germany) deal mainly with written and telephone communications monitoring within the framework of the G10 Act, the present case deals with the systematic surveillance of emails.

57 Millions of emails are sent and received every day. The monitoring of email traffic is easier than the monitoring of telephone conversations. Unlike with telephone conversations, the text of an email can be easily scanned for search terms. Simple technical procedures make it possible for the contents of millions of emails to be examined every day. This constitutes **mass surveillance**.

58 A key reason for the high number of hits is the fact that more than 12,000 content search terms are employed – a considerable number of them unspecific. The BND's "filter" is random and inadequate. If, for example, the search term "bomb" is used this can generate a large number of hits. Since the term can be used in all kinds of contexts, BND staff end up reading emails that have nothing to do with the threat of terrorism or crime in Germany. Moreover, the surveillance measures cover almost the entire globe. Finally, there is also a lack of quantitative restrictions that would create a sufficiently large sphere of protected communication, because contrary to its original intention and purpose the capacity criteria ("20%) is ineffective (see above, margin number 22 et seq.)

59 The scope of the "chilling effects" extends considerably beyond that of the actual surveillance. Owing to the lack of transparency and the ineffectual "abstract" limitation (area/capacity) citizens must assume that their international email traffic is being read by the BND.

60 In view of the limited amount of information deemed relevant for intelligence purposes relative to the number of "hits" and screened communications, the BND's strategic telecommunications surveillance methods must be considered groundless and disproportionate. They violated the applicant's right protected under Article 8, paragraph 1 of the ECHR.

c. No compensation through adequate remedy

61 All data gathered in the course of the surveillance measures is immediately deleted unless it is classified as relevant for intelligence purposes. The deletion of the data does not eliminate the infringement on freedom of telecommunications, but only covers up the traces (and creates an additional lack of transparency and increases the chilling effects). It deprives those affected of the possibility to provide reliable proof of the actual surveillance (see margin number 12 et seq.; margin number 66 et seq.)

62 The German courts nevertheless make legal remedy contingent on the complainant being able to prove that they were personally and directly affected by the measures, so that the lack of notification ultimately prevents any court examination of the case (contrary to the assumptions in the ECtHR Judgement of 6.9.1978, Application No 5029/71 – Klass and Others v. Germany; see margin number 6). The possibilities opened up by the G10 Commission for having the BND's activities in the area of strategic telecommunications surveillance subjected to review do not result in any compensation for the current deficits regarding an effective remedy, nor do they justify the encroachment on the right of the applicant under Article 8 of the ECHR (counter to the Federal Administrative Court judgement of 14.12.2016 – 6 A 2.15, margin number 27 et seq.) **(Annex 11, pp. 166-181)**. The possibility of filing an abstract complaint with the G10 Commission is ineffective (see margin number 19), particularly as the G10 Commission is not an independent supervisory authority given that it reviews orders which it has previously approved itself (before their execution) (see margin number 16).

3. Conclusion

63 In the light of the circumstances described above, the millions of intrusions on telecommunications secrecy are grossly disproportionate relative to the few hundred instrusions that are – at best – justified by relevance for intelligence purposes. The concrete figures demonstrate that the system used by the BND for strategic telecommunications surveillance, with its thousands of search terms, does not fulfil the criterion of "strict necessity", particularly as neither transparency nor the possibility for individual cases to be examined exists.

II. Violation of Article 10 of the ECHR

64 The applicant's right under Article 10, paragraph 1 of the ECHR was also violated. The right to freedom of expression includes the freedom to receive and impart information and ideas without interference by public authority and regardless of frontiers.

65 If a journalist is affected by infringements of Article 8 of the ECHR, as a rule his right under Article 10, paragraph 1 of the ECHR (cf. ECtHR Judgement of 29.6.2006, Application No 54934/00, § 145 – Weber and Saravia v. Germany) has also been infringed. The ECtHR ruled in *Weber and Saravia v. Germany* that the

G10 Act, in the version that applied at the time, provided adequate guarantees, so that there had been no violation of Article 8 of the ECHR and therefore no violation of Article 10 of the ECHR (ECtHR Judgement of 29.6.2006, Application No 54934/00, § 152 – Weber and Saravia v. Germany). If, however, the applicant's right under Article 8 of the ECHR has been violated, as explained in detail above, it follows that its right under Article 10 of the ECHR has also been violated (cf. also ECtHR Judgement of 22.11.2012, Application No 39315/06, §§ 89 ff. – Telegraaf Media Nederland Landelijke Medua B.V. and Others v. the Netherlands).

III. Violation of Article 13 of the ECHR

66 In addition, the applicant's right to an effective remedy under Article 13 of the ECHR is being violated, in that

- no notification of the recording and deletion of the majority of the screened communications is given;
- the public is, as a rule, informed about the measures only after even the protocol records documenting the deletion of the communications have already been deleted;
- the German courts make the admissibility of a complaint or constitutional complaint contingent on the complainant presenting concrete proof that they were affected, even though in practice it is impossible for the complainant to furnish such proof.

67 In accordance to Article 13 of the ECHR everyone whose recognised rights or freedoms are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity. In cases of **secret and arbitrary** surveillance in which those affected only learn about the **secret infringement of their fundamental rights** after the event, the guarantee of effective legal remedy is of particular importance. This must be taken into account in a legal system's provisions regarding effective remedy.

68 The applicant can assert (and did assert before the German courts (see margin number 36 et seq.) that there is a high probability that its right to freedom of communication – which is also protected by the ECHR – and its right pursuant to Article 8, paragraph 1 of the ECHR (see margin numver 43 et seq.) was infringed

secretly and without being notified, and that therefore it must be granted access to remedy (in the form of an effective complaint). The German Federal Administrative Court and the German Federal Constitutional Court refused to examine the complaint and constitutional complaint on their merits on the grounds that the applicant could not prove that it was directly affected, in other words, it could not prove that the BND had read or processed its emails (see margin number 387). With their decisions the German courts define an inapplicable – in that it is too narrowly interpreted – criterion (that also precludes effective remedy) as regards furnishing proof of being affected.

69 The Federal Administrative Court considered that there was no need for it to examine the matter of the probability of the applicant's emails being monitored by the BND, and took the view that only those whose communications have been classified as "relevant for intelligence purposes" have an effective right to complain – even though this small group of persons (118 in 2013) will, generally speaking, never learn of the monitoring, because Section 12 (1) of the G10 Act provides for numerous exemptions from the duty of notification.

70 The Federal Administrative Court and also the Federal Constitutional Court, should have come to the conclusion that it was probable that the applicant was affected by the monitoring, , and due to the high probability should have gone on to examine the surveillance measures on their lawfulness.

71 The Federal Administrative Court justified its decision pointing out that dismissing popular actions was in the legitimate interest of the public. With this argument, the Court fails to take into account that the very scale of the measures, and the resultant large number of people affected, results in a large number of potential complainants. If there is a large number of people affected, this does not make their legal actions popular actions.

72 In the *Camenzind v. Switzerland* case, the EctHR already determined that an effective legal remedy is not available when the requirements for substantiating the legitimacy of a complaint set by the case law of the responsible national courts are too stringent (ECtHR Judgement of 16.12.1997, Application No 136/1996/755/954, § 54 - Camenzind v. Switzerland). The subject of the aforementioned case was a house search. The Swiss Federal Court had declared the complaint inadmissible on the grounds that in accordance with Swiss case

law the complainant was not "presently affected". The Court found that the complainant did not have an "effective" legal remedy. It ruled that Article 13 of the ECHR had been violated, on account of the requirements for the substantiation of the complaint being too stringent.

73 The same must apply for the judgment of the German Federal Administrative Court and the decision of the German Federal Constitutional Court. The requirements of the Federal Administrative Court and the Federal Constitutional Court regarding the substantiation of secret surveillance are too stringent for the legal remedy to be considered effective within in the meaning of Article 13 of the ECHR. According to the criteria of the Federal Administrative Court and the Federal Constitutional Court, the right to effective remedy of those affected exists only on paper, and is therefore rendered inoperative.

74 If the decisions of the Federal Administrative Court and the Federal Constitutional Court were accepted as correct, no one whose email traffic is intercepted and processed by the BND would have any means of redress. If one considers that in 2013 alone more than 15,000 telecommunications were subjected to closer examination, of which only 118 were found to be relevant for intelligence, recourse to legal action is already **completely excluded** for those affected by the **more than 15,000 "hits".** The possibility of complaining to the G10 Commission does not represent an effective remedy within the meaning of Article 13 of the ECHR (see margin number 62).

75 The opinions of the Federal Administrative Court and the Federal Constitutional Court in the sensitive area of mass surveillance create an area in which there is no judicial remedy ("rechtsschutzfreier Raum") and therefore violate Article 13 of the ECHR. Moreover, the German courts contradict their own case law. In accordance with the case law of the Federal Constitutional Court, as regards the admissibility of a constitutional complaint in cases of secret infringements of basic rights, the complainant must merely establish that there is a **considerable probability** ("einiger wahrscheinlichkeit") that their fundamental rights have been infringed upon by measures that are based on the applied rules (Federal Constitutional Court, Judgement of 14.7.1999 — 1 BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95, margin number 146).

76 To ensure that Article 13 of the ECHR is not rendered inoperative, the requirements for a party to substantiate a claim of individual concern in cases of secret interference with a fundamental right are to be defined such that the affected party has access to effective remedy through the courts even when they cannot provide full proof that they were affected by restrictive measures. The German courts disregarded this and therefore created an area in which there is no judicial remedy. The applicant's right under Article 13 of the ECHR was therefore violated.

C. "Information about the exhaustion of domestic remedies and compliance with the time-limit set out in Article 35 Article 1")

77 The individual constitutional complaint is the last domestic legal remedy that was open to the applicant. The applicant submitted this complaint on 27.02.2017, within the one-month time limit that applies (see margin number 40), and thus exhausted the domestic legal remedies. The Federal Constitutional Court informed the applicant of its decision not to admit the complaint in a letter dated 30.5.2017 (cf. letter of 30.5.3017, **Annex 15, p. 239**), which the applicant received on 31.5.2017, so that the submission of the present application on 30.11.2017 complies with the six-month time limit pursuant to Article 35, paragraph 1 of the ECHR.