Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖB

Bern, 27. November 2014

Empfehlung

gemäss Art. 14 des Bundesgesetzes über das Öffentlichkeitsprinzip der Verwaltung

zum Schlichtungsantrag von

X
(Antragsteller)

gegen

Nachrichtendienst des Bundes NDB

I. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte stellt fest:

1. Der Antragsteller (Privatperson) hat am 20. Juni 2013 beim Nachrichtendienst des Bundes (NDB) gestützt auf das Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz, BGÖ; SR 152.3) ein Gesuch um Zugang zu einer „Liste der Namen und Versionsnummern aller Softwareprodukte […], welcher der NDB […] zur Erledigung aller seiner Tätigkeiten benötigt“ gestellt. Er bat weiter darum, in der Liste erkenntlich zu machen, welche der Softwareprodukte Eigenentwicklungen des NDB sind resp. welche Softwareprodukte im Auftrag des NDB erstellt wurden und zu welchen dieser Zugriff auf den Quellcode hat.

2. Mit Schreiben vom 2. Juli 2013 nahm der NDB Stellung zum Gesuch und teilte dem Antragsteller mit, dass der NDB einerseits von der Produktepalette der Führungsunterstützungsbasis (FUB) des VBS Gebrauch mache. Diese umfasse die allseits bekannten Anwendungen wie Word, Excel, Powerpoint usw. Andererseits betreibe der NDB weitere Applikationen, hinsichtlich derer er auf die einschlägige Gesetzgebung verweise, insbesondere auf die Verordnung über die Informationssysteme des Nachrichtendienstes des Bundes (ISV-NDB; SR 121.2). Soweit weitergehende diesbezügliche amtliche Dokumente bestehen sollten, wäre der Zugang aus Gründen der inneren oder äusseren Sicherheit der Schweiz sowie des Berufs-, Geschäfts- oder Fabrikationsgeheimnisses zu verweigern, weil eine Auflistung der Softwareprodukte Rückschlüsse auf allenfalls involvierte Firmen und deren technischen Know-how sowie auf die Arbeitsweise des NDB, vor allem jedoch auf die IKT-Sicherheitsarchitektur und damit allfällige Schwachstellen zulassen würde. Gleiches gelte für

Feldeggweg 1, 3003 Bern
Tel. 058 463 74 84, Fax 058 465 99 96
www.edoeb.admin.ch

den gewünschten Zugang zu Versionsnummern oder zu Angaben über den Zugriff auf Quellcodes.

3. Mit Schreiben vom 22. Juli 2013 reichte der Antragsteller einen Schlichtungsantrag gemäss Art. 13 BGÖ beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (Beauftragter) ein. Darin führte er aus, dass er nicht davon überzeugt sei, dass die Bekanntmachung dieser Informationen eine Gefahr für den NDB oder gar die Schweiz darstellen würde. Seiner Ansicht nach überwiege das öffentliche Interesse an diesen Informationen deutlich, insbesondere im Lichte der PRISM- oder Tempora-Enthüllungen.

4. Am 25. Juli 2013 bestätigte der Beauftragte dem Antragsteller den Eingang des Schlichtungsantrages und forderte zugleich den NDB auf, ihm alle relevanten Dokumente sowie eine ausführliche und detailliert begründete Stellungnahme einzureichen.

5. Nach gewährter Fristerstreckung reichte der NDB am 25. September 2013 eine Stellungnahme sowie die Korrespondenz mit dem Antragsteller ein und begründet die Zugangsverweigerung mit den Ausnahmebestimmungen von Art. 7 Abs. 1 Bst. c und g BGÖ. Er führte aus, dass der beim Nachrichtendienst eingesetzten Informatik bzw. deren Schutz eine hohe Bedeutung zukomme. In den letzten Jahren hätten gezielte Angriffe auf Informatikinfrastrukturen stark zugenommen. Gemäss NDB werde der Schutz der Systeme immer aufwändiger, weil fast bei jeder verwendeten Software früher oder später Schwachstellen und entsprechendes Schadenspotenzial entdeckt werde. Neben den allgemeinen Standardprogrammen komme spezifisch beim NDB eingesetzte Software zur Anwendung. Aus einer entsprechenden Auflistung liesse sich weitgehend die Informatikstruktur des NDB ableiten und eine Offenlegung derselben würde Tür und Tor für Angriffe öffnen. Die Gefahr gehe aber nicht alleine von der Kenntnis der Informatikstruktur als Ganzes aus, sondern ebenso von der Kenntnis einzelner Programme. So würde durch die Veröffentlichung von verwendeten Virenschutzprogrammen, Passwortsafes, Firewalls usw. das gesamte Informatiksicherheitskonzept offengelegt werden und damit wertlos gemacht. Der NDB weist weiter darauf hin, dass er über teilweise hochsensible Daten verfüge und es zu verhindern gelte, dass Angehörige von Lieferfirmen korrumpiert oder erpressbar gemacht würden, oder dass Angehörige fremder Nachrichtendienste in diese Firma eingeschleust werden könnten. Schliesslich gelte es zu beachten, dass die geschäftlichen Kontakte des NDB nicht offengelegt würden, auch weil sich daraus für die beteiligten Firmen Wettbewerbsvorteile oder –nachteile ergeben könnten.

6. Auf die weiteren Ausführungen des Antragstellers und des NDB sowie auf die eingereichten Unterlagen wird, soweit erforderlich, in den folgenden Erwägungen eingegangen.

II. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte zieht in Erwägung:

A. Formelle Erwägungen: Schlichtungsverfahren und Empfehlung gemäss Art. 14 BGÖ

7. Der Antragsteller hat ein Zugangsgesuch nach Art. 10 BGÖ beim NDB eingereicht und eine ablehnende Antwort erhalten. Als Teilnehmer an einem vorangegangenen Gesuchverfahren ist er zur Einreichung eines Schlichtungsantrages berechtigt. Der Schlichtungsantrag wurde formgerecht (einfache Schriftlichkeit) und fristgerecht (innert 20 Tagen nach Empfang der Stellungnahme der Behörde) beim Beauftragten eingereicht (Art. 13 BGÖ).

8. Das Schlichtungsverfahren kann auf schriftlichem Weg oder konferenziell (mit einzelnen oder allen Beteiligten) unter Leitung des Beauftragten stattfinden. Die Festlegung des Verfahrens im

Detail obliegt alleine dem Beauftragten.[1] Kommt keine Einigung zu Stande oder besteht keine Aussicht auf eine einvernehmliche Lösung, ist der Beauftragte gemäss Art. 14 BGÖ gehalten, aufgrund seiner Beurteilung der Angelegenheit eine Empfehlung abzugeben.

B. Materielle Erwägungen

9. Der Beauftragte prüft nach Art. 12 Abs. 1 der Verordnung über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsverordnung, VBGÖ, SR 152.31) die Rechtmässigkeit und die Angemessenheit der Beurteilung des Zugangsgesuches durch die Behörde. Er prüft damit im Schlichtungsverfahren einerseits beispielsweise, ob die für das Zugangsgesuch zuständige Behörde den Begriff des amtlichen Dokumentes (Art. 5 BGÖ) sowie die in Art. 7 f. BGÖ vorgesehenen Ausnahmeklauseln oder die Bestimmungen in Bezug auf den Schutz der Personendaten (Art. 9 BGÖ) rechtmässig angewendet hat. Andererseits prüft er in jenen Bereichen, in denen das Öffentlichkeitsgesetz der Behörde bei der Bearbeitung eines Zugangsgesuches einen gewissen Ermessensspielraum verleiht (z.B. Art der Einsichtnahme in amtliche Dokumente), ob die von der Behörde gewählte Lösung auf die Umstände des jeweiligen Falls abgestimmt und angemessen ist. Dabei kann der Beauftragte entsprechende Vorschläge im Rahmen des Schlichtungsverfahrens machen (Art. 12 Abs. 2 VBGÖ) oder gegebenenfalls eine entsprechende Empfehlung erlassen (Art. 14 BGÖ).[2]

10. Zur Begründung der Zugangsverweigerung stützt sich der NDB insbesondere auf Art. 7 Abs. 1 Bst. c BGÖ und stellt sich auf den Standpunkt, dass eine Offenlegung der verlangten Informationen die innere und äussere Sicherheit der Schweiz gefährden würde.

11. Art. 7 Abs. 1 Bst. c BGÖ ist darauf ausgerichtet, die öffentliche Sicherheit im weiteren Sinn zu schützen. Es ist selbstverständlich, dass ein Bekanntwerden bestimmter Informationen über polizeiliche oder nachrichtendienstliche Aktivitäten bestimmten Kreisen einen entscheidenden Vorteil einräumen kann.[3] Dies kann insbesondere für Einsatzdispositive der Streitkräfte, Einsatzmethoden derjenigen Verwaltungseinheiten, die mit Terrorismusbekämpfung beauftragt sind, die Pläne von Verteidigungs- oder Überwachungsanlagen, die technischen Daten zu Ausrüstung und Bewaffnung, die Analysen der Nachrichtendienste und die Planung von Massnahmen zur Versorgung oder Information der Bevölkerung im Krisenfall gelten.[4] Eine Gefährdung der öffentlichen Sicherheit ist dann anzunehmen, wenn das Bekanntwerden bestimmter Dokumente und Informationen ein erhöhtes Risiko von Angriffen zur Folge hätte[5] (z.B. Sicherheitsbeurteilungen und Massnahmenpläne der Behörden[6], Informationen über die Organisation, die Tätigkeit und Strategie von Behörden namentlich in Bezug auf Sicherheitsaufgaben[7]). Trotzdem rechtfertigen die Sicherheitszwecke nicht alles und jedes geheim zu halten.[8] Besonders aktuelle Bedrohungen können entscheidend für die Einschätzung der Frage sein, ob die Herausgabe eines Dokuments die öffentliche Sicherheit ernsthaft gefährden könnte.[9] Es ist festzuhalten, dass die Offenlegung der verwendeten Softwarepalette

---

1 BBl 2003 2024.

2 CHRISTINE GUY-ECABERT, in: Brunner/Mader [Hrsg.], Stämpflis Handkommentar zum BGÖ, Art. 13, Rz 8.

3 BBl 2003 2009 ; Basler Kommentar zum Öffentlichkeitsgesetz, URS STEIMEN, Art. 7 N 21, 3. Aufl., Basel 2014.

4 BERTIL COTTIER/RAINER J. SCHWEIZER/NINA WIDMER, in Brunner/Mader [Hrsg.], Stämpflis Handkommentar zum BGÖ, Art. 7 Rz. 27.

5 BSK BGÖ, URS STEIMEN, Art. 7 N 22.

6 Empfehlung EDÖB vom 21. Oktober 2010: VBS / Sicherheitsbericht „Islamistische Imame“, Ziffer II.B.10 ff.

7 Empfehlung EDÖB vom 18. November 2010: VBS / Inspektionsberichte ND-Aufsicht, Ziffer II.B.10.2.

8 COTTIER/SCHWEIZER/WIDMER, a.a.O., Rz 28.

9 BSK BGÖ, URS STEIMEN, a.a.O. ; COTTIER/SCHWEIZER/WIDMER, a.a.O.

nicht für jedes Softwareprodukt und auch nicht für jede Behörde ein Sicherheitsproblem darstellen dürfte. Ein solches ergibt sich primär für Behörden, die im Fokus von Cyber-Kriminellen stehen und staatliche Sicherheitsaufgaben wahrnehmen sowie wenn durch die Offenlegung Schlüsse auf sicherheitsrelevante Schwachstellen gezogen werden können.[10]

12. Der Beauftragte ist mit dem NDB einig, dass mit dem Bekanntwerden der Namen sowie der Versionsnummern der Software im vorliegenden Fall ausländische Nachrichtendienste wie auch private Informatikspezialisten die Schwachstellen dieser Softwareprodukte für ihre eigenen Zwecke ausnutzen könnten. Zudem kann nicht ausgeschlossen werden, dass mit diesen Kenntnissen Lieferfirmen korrumpiert oder sonst wie erpressbar gemacht würden oder gar fremde Nachrichtendienste diese Firmen ins Visier nehmen könnten. Zudem könnte die Kenntnis einzelner eingesetzter Programme wie Virenschutzprogramme, Passwortsafes, Firewalls usw. die sicherheitsrelevanten Teile des Informatiksicherheitskonzepts des NDB offenlegen und dadurch wirkungslos machen. Dies kann durchaus zu einer höheren Gefährdung der inneren oder äusseren Sicherheit der Schweiz führen. Gleiches gilt für die Angaben bezüglich Zugriff auf die Quellcodes.

13. Heutzutage werden Spionagemittel anderer Länder und Cyberkriminalität immer bedeutender. Das Zugänglichmachen von Informationen über die vom NDB eingesetzten Informatiksysteme könnte das Risiko von Angriffen ernsthaft erhöhen und seine Aufgabenerfüllung empfindlich beeinträchtigen. Der Aspekt der Informatiksicherheit des NDB steht nach Ansicht des Beauftragten in einem direkten Bezug zur inneren und äusseren Sicherheit der Schweiz. Zudem verfügt der NDB sowohl über teilweise hochsensible Daten aus dem Bereich der inneren und äusseren Sicherheit der Schweiz als auch über besonders schützenswerte Personendaten i.S.v. Art. 3 Bst. c des Bundesgesetzes über den Datenschutz (Datenschutzgesetz, DSG; SR 235.1). Damit erachtet der Beauftragte die Intensität der Gefährdung vorliegend als gegeben.

14. Diese Erwägungen gelten jedoch nicht hinsichtlich der verwendeten Standardanwendungen (vom NDB als BURAUT bezeichnet), da diese nicht explizit mit der Kerntätigkeit des NDB zusammenhängen, sondern in der ganzen Bundesverwaltung zum Einsatz kommen.

15. Folglich sind nach Ansicht des Beauftragten die Voraussetzungen von Art. 7 Abs. 1 Bst. c BGÖ hinsichtlich der spezifisch beim NDB eingesetzten Software erfüllt. Demgegenüber ist das Verzeichnis der Standardprogramme (inkl. Versionsnummern) zugänglich zu machen.

16. Da nach Ansicht des Beauftragten die Ausnahmebestimmung von Art. 7 Abs. 1 Bst. c BGÖ vorliegend zur Anwendung gelangt, kann die Frage, ob zusätzlich auch die Ausnahme von Art. 7 Abs. 1 Bst g BGÖ anwendbar ist, offen bleiben.

17. Zusammengefasst gelangt der Beauftragte damit zu folgendem Ergebnis:
Der NDB gewährt den Zugang zu der Liste der Standardsoftware (BAB), inkl. Versionsnummern. Für die übrigen vom Antragsteller verlangten Informationen hält er an seiner Zugangsverweigerung fest (Art. 7 Abs. 1 Bst. c BGÖ).

III. Aufgrund dieser Erwägungen empfiehlt der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte:

18. Der Nachrichtendienst des Bundes gewährt den Zugang zur Liste mit der Standardsoftware (BURAUT), inkl. den Versionsnummern.

19. Der Nachrichtendienst des Bundes hält an seiner Verweigerung zu den übrigen mit

[10] Bundesbeauftragte für Datenschutz und Informationsfreiheit (BFDI), 4. Tätigkeitsbericht zur Informationsfreiheit, S. 42.

Zugangsgesuch verlangten Dokumenten fest (Art. 7 Abs. 1 Bst. c BGÖ).

20. Der Nachrichtendienst des Bundes erlässt eine Verfügung nach Art. 5 des Bundesgesetzes über das Verwaltungsverfahren (VwVG, SR 172.021), wenn er in Abweichung von Ziffer 18 den Zugang nicht gewähren will.

21. Der Nachrichtendienst des Bundes erlässt die Verfügung innert 20 Tagen nach Empfang dieser Empfehlung (Art. 15 Abs. 3 BGÖ).

22. Der Antragsteller kann innerhalb von 10 Tagen nach Erhalt dieser Empfehlung beim Nachrichtendienst des Bundes den Erlass einer Verfügung nach Art. 5 VwVG verlangen, wenn er mit der Empfehlung nicht einverstanden ist (Art. 15 Abs. 1 BGÖ).

23. Gegen die Verfügung kann der Antragsteller beim Bundesverwaltungsgericht Beschwerde führen (Art. 16 BGÖ).

24. Diese Empfehlung wird veröffentlicht. Zum Schutz der Personendaten der am Schlichtungsverfahren Beteiligten wird der Name des Antragstellers anonymisiert (Art. 13 Abs. 3 VBGÖ).

25. Die Empfehlung wird eröffnet:

- X

- Nachrichtendienst des Bundes NDB
  Papiermühlestrasse 20
  3003 Bern

Hanspeter Thür