Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖB

Bern, 26. November 2014

Empfehlung

gemäss Art. 14 des Bundesgesetzes über das Öffentlichkeitsprinzip der Verwaltung

zum Schlichtungsantrag von

X
(Antragsteller)

gegen

Dienst Überwachung Post- und Fernmeldeverkehr ÜPF

I. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte stellt fest:

1. Der Antragsteller (Privatperson) hat am 20. Juni 2013 beim Dienst Überwachung Post- und Fernmeldeverkehr (Dienst ÜPF) 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 Dienst ÜPF[…] zur Erledigung aller seiner Tätigkeiten benötigt“ gestellt. Er bat weiter darum, in der Liste erkenntlich zu machen, welche der Softwareprodukte Eigenentwicklungen des Dienstes ÜPF sind resp. Welche Softwareprodukte im Auftrag des Dienstes ÜPF erstellt wurden und zu welchen der Dienst Zugriff auf den Quellcode hat. Zu den Aufgaben des Dienstes ÜPF gehört es u.a., auf Anordnung der Strafverfolgungsbehörden Post- und Fernmeldeüberwachungen durchzuführen. Er holt dafür bei den Fernmeldedienstanbieterinnen jene Daten ein, welche die Strafverfolgungsbehörden anfordern, um Straftaten aufzuklären.[1]

2. Am 24. Juni 2013 bestätige der Dienst ÜPF dem Antragsteller per E-Mail u.a., dass tatsächlich ein oder mehrere Inventare über diejenige Software, welche der Dienst einsetze oder welche für den Dienst eingesetzt würden, bestünden. Weiter führte er aus, dass das gesamte Software-Inventar des Dienstes ÜPF höchst sensibel sei. Aus Gründen des Datenschutzes sowie des Schutzes des Fernmeldegeheimnisses sei es unter allen Umständen zu vermeiden, dass

[1] https://www.li.admin.ch/de/ptss/index.html; Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF, SR 780.1).

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

Personen, welche nicht im oder für den Dienst ÜPF tätig seien, Kenntnis davon hätten, mit welcher Software der Dienst ÜPF arbeite. Dies würde allfällige Angriffe auf die Systeme des Dienstes ÜPF erleichtern. Damit wäre nach Art. 7 Abs. 1 Bst. b BGÖ die zielkonforme Durchführung konkreter behördlicher Massnahmen („nämlich die Überwachungen und der Schutz der Daten in unseren Systemen") gefährdet. Zudem wären gemäss Art. 7 Abs. 1 Bst. e BGÖ wohl auch die Beziehungen des Bundes zu den Kantonen bzw. den Strafverfolgungsbehörden der Kantone beeinträchtigt, welche nach Ansicht des Dienstes ÜPF wohl kaum Verständnis für die Bekanntgabe derlei sensibler Daten im Bereich der Strafverfolgung haben dürften. Des Weiteren erscheine auch die innere Sicherheit gemäss Art. 7 Abs. 1 Bst. c BGÖ gefährdet.

3. Mit E-Mail vom 24. Juni 2013 teilte der Antragsteller dem Dienst ÜPF mit, dass durch „Security by Obscurity" die Sicherheit des Dienstes gefährdet werde, und er überzeugt sei, dass die Öffentlichkeit ein Bedürfnis und Recht habe zu wissen, welche Software der Dienst einsetze, denn so könne der unabhängige Dritte beurteilen, über welche Möglichkeiten der Datenbearbeitung resp. Überwachung der Dienst verfüge.

4. Mit Schreiben vom 27. Juni 2013 reichte der Antragsteller einen Schlichtungsantrag gemäss Art. 13 BGÖ beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (Beauftragter) ein.

5. Am 1. Juli 2013 bestätigte der Beauftragte dem Antragsteller den Eingang seines Schlichtungsantrages und forderte zugleich den Dienst ÜPF auf, ihm alle relevanten Dokumente sowie eine ausführliche und detailliert begründete Stellungnahme einzureichen.

6. Am 5. Juli 2013 reichte der Dienst ÜPF dem Beauftragten eine Stellungnahme und die relevanten Dokumente ein. Diese Stellungnahme deckte sich grundsätzlich mit jener an den Antragsteller vom 24. Juni 2013 (s. Ziff. 2). Ergänzend hielt der Dienst fest, es gebe – entgegen seiner Antwort vom 24. Juni 2013 an den Antragsteller – keine bestehenden Listen. Die Erstellung der entsprechenden Verzeichnisse sei zwar möglich, dafür würden jedoch insgesamt 27 Stunden benötigt, wofür entsprechend der Verordnung über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsverordnung, VBGÖ, SR 152.31) eine Gebühr von mindestens CHF 2700.- in Rechnung gestellt werden müsste. Der Dienst ÜPF zeigte sich gegenüber dem Beauftragten bereit, die Standardsoftware (Büroautomation Bund, BAB)[2], die auf allen individuellen Arbeitsplätzen eingesetzt werde, gegenüber der Öffentlichkeit offenzulegen. Eine Offenlegung des Software-Inventars, welches zur Umsetzung der strafprozessualen Überwachungsmassnahmen eingesetzt werde, sei allerdings höchst sensibel, da bereits der Name der verwendeten Software ein Mosaikstein sei, der dazu beitrage, die Sicherheit der eingesetzten Informatiksysteme zu garantieren. Bereits die Bekanntgabe der einzelnen Produktenamen könnte allfällige gezielte Angriffe erleichtern und damit die Sicherheit der Systeme des Dienstes ernsthaft gefährden. Damit wäre auch ein Grossteil der Strafverfolgung schwerster Kriminalität in der Schweiz empfindlich gefährdet, weil die Fernmeldeüberwachung unter Umständen schweizweit für eine gewisse Zeit nicht mehr funktionieren würde.
Zudem rechne der Dienst damit, dass Kriminelle Rückschlüsse auf die Ermittlungstaktik bzw. nicht überwachbare Kommunikationskanäle ziehen könnten, wodurch die Fernmeldeüberwachung in gewissen Teilen unbrauchbar würde. Aufgrund dieser Ausführungen sei, so der Dienst ÜPF, die zielkonforme Durchführung konkreter behördlicher Massnahmen (Art. 7 Abs. 1 Bst. b BGÖ) von Bund und Kantonen, nämlich die Überwachung und der Schutz der Daten in den Systemen seines Dienstes, gefährdet.

---

[2] Für BAB sind zwei ISB-Standards definiert, A029 BAB Client SW und A033 BAB Server SW und Services", http://www.bit.admin.ch/abkvz/index.html?action=id&id=547&pos=1&abrlang=de&lang=fr.

Ergänzend sah der Dienst ÜPF durch die Bekanntgabe entsprechender Listen die innere und äussere Sicherheit der Schweiz gefährdet (Art. 7 Abs. 1 Bst. c BGÖ), da auch ausländische Nachrichtendienste potentielle Angreifer der Systeme des Dienstes ÜPF seien und die entsprechenden Schwachstellen ausnützen könnten.
Schliesslich erachtete der Dienst ÜPF eine Beeinträchtigung der Beziehungen zu den kantonalen Strafverfolgungsbehörden als gegeben (Art. 7 Abs. 1 Bst. e BGÖ).

7. Auf die weiteren Ausführungen des Antragstellers und des Dienstes ÜPF 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

8. Der Antragsteller hat ein Zugangsgesuch nach Art. 10 BGÖ beim Dienst ÜPF 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).

9. 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.[3] 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

10. 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).[4]

11. Der Dienst ÜPF ist eine Verwaltungseinheit der dezentralen Bundesverwaltung gemäss Art. 7a Abs. 1 Bst. b der Regierungs- und Verwaltungsorganisationsverordnung (RVOV, SR 172.010, s.a. Anhang 1). Er ist dem Informatik Service Center des Eidgenössischen Justiz- und

---

[3] BBl 2003 2024.

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

Polizeidepartements (ISC-EJPD) administrativ zugeordnet. Als Teil der Bundesverwaltung fällt der Dienst ÜPF unter den Geltungsbereich des Öffentlichkeitsgesetzes (Art. 2 Abs. 1 Bst. a BGÖ). Daher gelten das Öffentlichkeitsprinzip und seine Ausnahmen (Art. 7 ff. BGÖ) für alle amtlichen Dokumente, die sich in seinem Besitz befinden (Art. 5 BGÖ).

12. In seiner Stellungnahme vom 5. Juli 2013 an den Beauftragten präzisierte der Dienst ÜPF, dass keine Verzeichnisse existierten, welche die gesamten verlangten Informationen enthielten. Gleichzeitig zeigte er sich indes bereit, ein Verzeichnis mit der an den individuellen Arbeitsplätzen eingesetzten Standardsoftware (BAB) zugänglich zu machen.

13. *Der Dienst ÜPF erstellt das Verzeichnis der Standardsoftware (inkl Versionsnummern) und macht sie dem Antragsteller zugänglich.*

14. Keinen Zugang will der Dienst ÜPF zum Inventar derjenigen Software gewähren, welche für die Umsetzung der strafprozessualen Überwachung eingesetzt wird. Zur Begründung der Zugangsverweigerung stützt sich der Dienst ÜPF insbesondere auf Art. 7 Abs. 1 Bst. b BGÖ und stellt sich auf den Standpunkt, dass eine Offenlegung der verlangten Informationen die zielkonforme Durchführung konkreter behördlicher Massnahmen von Bund und Kantonen, nämlich die Überwachung und der Schutz der Daten in den Systemen des Dienstes ÜPF, beeinträchtigen würde. Mit anderen Worten befürchtet der Dienst ÜPF durch die Offenlegung des Software-Inventars einerseits eine Gefährdung der Sicherheit seiner Informatiksysteme durch mögliche Angriffe und andererseits sieht er die wirksame Post- und Fernmeldeüberwachung gefährdet.

15. Gemäss der Botschaft zum Öffentlichkeitsgesetz dient diese Ausnahmebestimmung dazu, Informationen geheim zu halten, die der Vorbereitung konkreter behördlicher Massnahmen dienen. Die Ausnahme kann immer dann angerufen werden, wenn durch die Zugänglichmachung bestimmter Informationen, eine Massnahme teilweise oder völlig vereitelt würde.[5] Als Beispiele geschützter behördlicher Massnahmen nennen Botschaft und Lehre etwa Aufsichtsmassnahmen, Inspektionen der Steuerbehörden, Aufklärungs- und Präventionskampagnen, behördliche Ermittlungen oder administrative Überwachungen.[6]

16. Da sich mit Art. 7 Abs. 1 Bst. b BGÖ theoretisch ein Grossteil aller Zugangsgesuche verweigern liesse, wird die Ausnahmebestimmung in der Lehre als eigentlicher Blankocheck kritisiert, welcher die Gefahr birgt, das Öffentlichkeitsgesetz seines Inhalts zu berauben.[7] Das Bundesverwaltungsgericht hat festgehalten, dass die wörtliche Anwendung von Art. 7 Abs. 1 Bst. b BGÖ dazu führen würde, dass praktisch sämtliche Informationen dem Zugang entzogen werden könnten: „Deshalb ist es wichtig, dass die Ausnahmebestimmung nur eingesetzt wird, wenn die Offenlegung der durchzuführenden Massnahmen deren Erfolg ernsthaft gefährdet. Mit anderen Worten, die Geheimhaltung dieser Vorkehrungen muss der Schlüssel zu ihrem Erfolg darstellen“.[8] Im Ergebnis soll die Ausnahmebestimmung sicherstellen, dass sich Bürgerinnen und Bürger an das Gesetz halten und die Behörden die Quellen der erhaltenen Auskünfte sowie ihre Kontroll-, Aufsichts- oder Überwachungsmethoden nicht preisgeben müssen, sofern dadurch eine konkrete, geplante Massnahme wirkungslos würde oder die Betroffenen ihr Verhalten änderten, um den Überwachungen zu entgehen.[9]

---

5 BBl 2003 2009.

6 Empfehlung EDÖB vom 18. Februar 2014: METAS / Datenbank Labor Verkehr, II.B.23.

7 BERTIL COTTIER/ RAINER J. SCHWEIZER/NINA WIDMER, in: Brunner/Mader [Hrsg.], Stämpflis Handkommentar zum BGÖ, Art. 7, Rz 24.

8 Urteil des BVGer A-3443/2010 vom 18. Oktober 2010 E. 5.2 ; COTTIER/SCHWEIZER/WIDMER, a.a.O.

9 Empfehlung EDÖB vom 17. September 2013: BAZL / Monitoring Nachtflugverkehr am Flughafen Zürich, Ziffer II.B.29 ; COTTIER/SCHWEIZER/WIDMER, a.a.O., Rz 25.

17. Wie einleitend dargelegt (s. Ziff. 1), betrifft die Haupttätigkeit des Dienstes ÜPF die Post- und Fernmeldeüberwachungen im Rahmen von Strafverfolgungen, wozu er eine Reihe von spezifischen Softwareprodukten einsetzt. Nach Ansicht des Beauftragten hat der Dienst ÜPF in diesem konkreten Fall nachvollziehbar dargelegt, weshalb die Software, welche zur Umsetzung der strafprozessualen Überwachungsmassnahmen eingesetzt wird, nicht zugänglich gemacht werden darf. Die Offenlegung aller vom Dienst ÜPF genutzter Softwareprodukte würde es erlauben, sich ein umfassendes Bild über ihre Ermittlungsmethodik und die technischen Möglichkeiten sowie die Grenzen der Überwachungen zu machen. Es wäre dadurch für interessierte bzw. betroffene Personen möglich, auf nicht überwachbare Kommunikationskanäle auszuweichen, um sich einer Überwachung des Dienstes ÜPF zu entziehen, wodurch der Erfolg dieser Massnahme infrage gestellt wird. Soweit der Beauftragte dies beurteilen kann, erscheint es zudem plausibel, dass die Kenntnis gewisser Informationen (z.B. Firewall, Antivirusprogramme) Angriffe auf das Informationssystem des Dienstes ÜPF erleichtern würden, da dadurch potentielle Schwachstellen erkennbar und ausnutzbar würden, wodurch die Überwachungsmassnahmen ebenfalls gefährdet würden.

18. Grundsätzlich reicht eine rein theoretisch mögliche Beeinträchtigung nicht aus, um die Ausnahmebestimmung zu Recht geltend zu machen. Es muss ein ernsthaftes Risiko bestehen, dass die Beeinträchtigung eintritt.[10] Angesichts der Tatsache, dass das Überwachungssystem des Dienstes ÜPF das Kernstück seiner Tätigkeit darstellt sowie wesentlicher Bestandteil seiner gesetzlichen Aufgabenerfüllung ist und der Dienst ÜPF dadurch stärker im Fokus steht als andere Behörden, erachtet der Beauftragte die Intensität der Gefährdung vorliegend als gegeben. Würde dieses Überwachungssystem gefährdet, könnte der Dienst ÜPF seine Aufgaben nicht mehr zielkonform wahrnehmen.

19. *Aus diesem Grund sind im vorliegenden Fall die Voraussetzungen von Art. 7 Abs. 1 Bst. b BGÖ erfüllt.*

20. Diese Ausführungen gelten nach Ansicht des Beauftragten auch für die Versionsnummern der sensiblen Softwareprogramme und die Quellcodes. In Bezug auf Letztere hat der Dienst ÜPF immerhin festgehalten, dass bei eigens für ihn erstellte und programmierte Software die Allgemeinen Geschäftsbedingungen des Bundes für Werkverträge im Informatikbereich und die Pflege von Individualsoftware, Kapitel 7.3, gelten. Demnach muss der Lieferant dem Besteller für die Individualsoftware den Quellcode, inklusive der für dessen Bearbeitung notwendigen Informationen und Dokumentationen, liefern.[11]

21. Da nach Ansicht des Beauftragten die Ausnahmebestimmung von Art. 7 Abs. 1 Bst. b BGÖ vorliegend zur Anwendung gelangt, kann die Frage, ob zusätzlich auch die Ausnahmen von Art. 7 Abs. 1 Bst c und e BGÖ anwendbar sind, offen bleiben.

22. *Zusammengefasst gelangt der Beauftragte damit zu folgendem Ergebnis:*
Der Dienst ÜPF 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. b BGÖ).

---

[10] COTTIER/SCHWEIZER/WIDMER, a.a.O., Rz 4.

[11] http://www.bbl.admin.ch/bkb/02617/02618/02625/index.html?lang=de&download=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1acy4Zn4Z2qZpnO2Yuq2Z6gpJCDfIB2fmym162epYbg2c_JjKbNoKSn6A--.

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

23. Der Dienst Überwachung Post- und Fernmeldeverkehr gewährt den Zugang zur Liste mit der Standardsoftware (BAB), inkl. den Versionsnummern.

24. Der Dienst Überwachung Post- und Fernmeldeverkehr hält an seiner Verweigerung zu den übrigen mit Zugangsgesuch verlangten Dokumenten fest (Art. 7 Abs. 1 Bst. b BGÖ).

25. Der Dienst Überwachung Post- und Fernmeldeverkehr erlässt eine Verfügung nach Art. 5 des Bundesgesetzes über das Verwaltungsverfahren (VwVG, SR 172.021), wenn er in Abweichung der Ziffer 23 den Zugang nicht gewähren will.

26. Der Dienst Überwachung Post- und Fernmeldeverkehr erlässt die Verfügung innert 20 Tagen nach Empfang dieser Empfehlung (Art. 15 Abs. 3 BGÖ).

27. Der Antragsteller kann innerhalb von 10 Tagen nach Erhalt dieser Empfehlung beim Dienst Überwachung Post- und Fernmeldeverkehr den Erlass einer Verfügung nach Art. 5 VwVG verlangen, wenn er mit der Empfehlung nicht einverstanden ist (Art. 15 Abs. 1 BGÖ).

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

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

30. Die Empfehlung wird eröffnet:

- X

- Informatik Service Center ISC-EJPD
  Dienst Überwachung Post- und Fernmeldeverkehr ÜPF
  Fellerstrasse 15
  3003 Bern

Hanspeter Thür