EDOEB empfehlung-vom-15-mai-2020-isb-berichte-informatiksicherheit-bund-2014-2018entkl-2020-05-15 vom 15. Mai 2020

EDÖB, 2020-05-15, DE

Quelle: https://mcp.opencaselaw.ch/entscheid/edoeb_empfehlung-vom-15-mai-2020-isb-berichte-informatiksicherheit-bund-2014-2018entkl-2020-05-15

FR: EDOEB
empfehlung-vom-15-mai-2020-isb-berichte-informatiksicherheit-bund-2014-2018entkl-2020-05-15 du 15 mai 2020

IT: EDOEB
empfehlung-vom-15-mai-2020-isb-berichte-informatiksicherheit-bund-2014-2018entkl-2020-05-15 del 15 maggio 2020

Erwägungen

E. 1

Der Antragsteller (Journalist) hat Mitte Mai 2019 gestützt auf das Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz, BGÖ; SR 152.3) beim Informatiksteuerungsorgan des Bundes (ISB) ein (erstes) Gesuch um Zugang zu den Berichten "Informatiksicherheit Bund" für die Jahre 2014-2018 eingereicht. Das ISB verweigerte den Zugang gestützt auf die Ausnahmebestimmung der Gefährdung der inneren und äusseren Sicherheit der Schweiz (Art. 7 Abs. 1 Bst. c BGÖ). Am 14. Juni 2019 fand eine Schlichtungssitzung statt, in der sich die Parteien einigen konnten. Im Nachgang zur Schlichtungssitzung und entsprechend der erzielten Einigung erstellte das ISB den Bericht "Stand der Informatiksicherheit in der Bundesverwaltung 2018", den es dem Antragsteller am 14. Oktober 2019 zustellte und gleichentags im Internet veröffentlichte.1 In der Folge stellte der Antragsteller dem ISB am 18. Oktober 2019 zusätzlich eine Reihe von Fragen per E-Mail, die es am selben Tag beantwortete.

E. 2

Der Antragsteller war mit dem veröffentlichten Bericht "nicht vollständig zufrieden […], da er mein in der Schlichtungsverhandlung formuliertes Anliegen nicht erfüllt, einen Überblick zu erhalten, welche Bundesämter bzw. Departemente die Weisungen zur IKT-Sicherheit des Bundes einhalten". Darum reichte der Antragsteller am 27. Dezember 2019 gestützt auf das Öffentlichkeitsgesetz beim ISB erneut ein Gesuch um Zugang zu den Berichten "Informatiksicherheit Bund" von 2014 bis 2018 (nachfolgend Berichte) ein. Für den Fall, dass "die Informationen nicht in den obigen Berichten enthalten sind", verlangte er zusätzlich verschiedene Übersichten (nachfolgend Übersichten): - "Eine Übersicht 2014-2019 über den Stand von Umsetzung und Kontrolle der Informatiksicherheitsvorgaben aufgeschlüsselt nach Verwaltungseinheiten bzw. Departementen (wie es die Departemente gemäss der strukturierten Umfrage zum

1 https://www.isb.admin.ch/dam/isb/de/dokumente/Dokumentation/berichte/Stand-Informatiksicherheit-Bundesverwaltung-2018.pdf.download.pdf/Stand-Informatiksicherheit-Bundesverwaltung-2018.pdf (zuletzt besucht am 15.05.2020)

Jahresende dem ISB berichten; Kap. 2 im Bericht «Stand der Informatiksicherheit in der Bundesverwaltung 2018») - Eine Übersicht 2014-2019 über die Anzahl der Sicherheitsvorfälle aufgeschlüsselt nach Art des Ereignisses sowie nach Verwaltungseinheiten bzw. Departementen und (Kap. 4) - Eine Übersicht 2014-2019 über die Anzahl von Malware infizierten Rechnern (Arbeitsplatzgeräte, Server, Netzwerkkomponenten) aufgeschlüsselt nach Verwaltungseinheiten bzw. Departementen (Kap. 4.1) - Eine Übersicht 2014-2019 über die Anzahl und Art der Internen Störungen und Vorkommnisse aufgeschlüsselt nach Verwaltungseinheiten bzw. Departementen (Kap. 4.3)"

E. 3

Mit E-Mail vom 20. Januar 2020 lehnte das ISB die Herausgabe der verlangten Berichte erneut mit Verweis auf die Gefährdung der inneren oder äusseren Sicherheit der Schweiz gemäss Art. 7 Abs. 1 Bst. c BGÖ ab. Das ISB führte weiter aus, dass es der Einigung vollumfänglich nachgekommen sei und die Nachfragen des Antragstellers vom 18. Oktober 2019 entsprechend beantwortet habe. Zu den verlangten Übersichten äusserte sich das ISB nicht.

E. 4

Am 30. Januar 2020 reichte der Antragsteller einen Schlichtungsantrag beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (Beauftragter) ein.

E. 5

Mit Schreiben vom 31. Januar 2020 bestätigte der Beauftragte gegenüber dem Antragsteller den Eingang des Schlichtungsantrages und forderte das ISB dazu, die betroffenen Dokumente sowie bei Bedarf eine ergänzende Stellungnahme einzureichen.

E. 6

Am 21. Februar 2020 reichte das ISB die betroffenen Dokumente, jedoch keine ergänzende Stellungnahme ein.

E. 7

Eine bereits angesetzte Schlichtungssitzung wurde auf Antrag des Antragstellers zweimal verschoben. Die Sitzung wurde schliesslich aufgrund der Massnahmen des Bundesrates in Bezug auf Covid-19 storniert und das Schlichtungsverfahren wurde schriftlich durchgeführt. Aus diesem Grund räumte der Beauftragte am 16. März 2020 dem Antragsteller und dem ISB nochmals die Gelegenheit ein, eine ergänzende Stellungnahme einzureichen.

E. 8

In seiner Stellungnahme vom 20. März 2020 erklärte der Antragsteller im Wesentlichen, dass er Zugang zu allen Berichten haben möchte, um nachvollziehen zu können, "wie die Situation in den einzelnen Verwaltungseinheiten insbesondere bezüglich Umsetzung der Vorgaben aussieht" und insbesondere "welche Verwaltungseinheiten sich wie gut an die Vorgaben des ISB haben[sic]". Er führte dazu u.a. aus, dass an diesen Angaben ein öffentliches Interesse bestehe, denn "wenn sich Bundesstellen in einem so heiklen Bereich wie der Cybersicherheit nicht an die Weisungen des ISB halten, stellen sich Fragen des Funktionierens der Verwaltung in diesem Bereich. Es stellt sich die Frage, wie gut der Bund vor den Cyberrisiken geschützt ist. Für diese Beurteilung ist auch wichtig zu wissen, welche

Verwaltungseinheiten wie oft von Angriffen oder Störungen betroffen waren. Nur mit diesen Informationen kann sich die Öffentlichkeit ein Bild über den Stand der Informatiksicherheit des Bundes machen."

E. 9

Am 23. März 2020 reichte das ISB dem Beauftragten seine ergänzende Stellungnahme ein. In Bezug auf die Berichte 2014-2018 des Zugangsgesuches wiederholte das ISB die in seiner Stellungnahme vom 20. Januar 2020 an den Antragsteller dargelegten Argumente. Betreffend die Übersichten 2014-2019 führte es aus, dass "[d]er Bericht «Informatiksicherheit Bund 2019» […] in Vorbereitung [ist]. Der Bundesrat hat den Bericht daher noch nicht zur Kenntnis nehmen können. Nach Art. 8 Abs. 2 BGÖ dürfen amtliche Dokumente erst dann zugänglich gemacht werden, wenn der politische Entscheid, für den sie die Grundlage darstellen, getroffen ist. Da sich das Gesuch […] auf Daten des Jahres 2019 bezieht, die in den vom Bundesrat vorzulegenden Bericht «Informatiksicherheit Bund 2019» aufgenommen werden soll, muss das

Gesuch abgelehnt werden." Die Behörde informierte den Beauftragten weiter darüber, dass sie für die Öffentlichkeit einen Bericht über den Stand der "Informatiksicherheit in der Bundesverwaltung 2019" erstellen und dass dieser Bericht so weit wie möglich die Anträge des Antragstellers berücksichtigen werde.

E. 10

Auf die weiteren Ausführungen des Antragstellers und des ISB 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

E. 11

Der Antragsteller reichte ein Zugangsgesuch nach Art. 10 BGÖ beim ISB ein. Dieses verweigerte den Zugang zu dem verlangten Dokument. Der Antragsteller ist als Teilnehmer an einem vorangegangenen Gesuchsverfahren zur Einreichung eines Schlichtungsantrags berechtigt (Art. 13 Abs. 1 Bst. a BGÖ). Der Schlichtungsantrag wurde formgerecht (einfache Schriftlichkeit) und fristgerecht (innert 20 Tagen nach Empfang der Stellungnahme der Behörde) beim Beauftragten eingereicht (Art. 13 Abs. 2 BGÖ).

E. 12

Das Schlichtungsverfahren findet auf schriftlichem Weg oder konferenziell (mit einzelnen oder allen Beteiligten) unter Leitung des Beauftragten statt, der das Verfahren im Detail festlegt.2 Kommt keine Einigung zustande 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

E. 13

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.3

E. 14

Das ISB macht in seiner Stellungnahme vom 20. Januar 2020 an den Antragsteller geltend, dass "[d]ie Verwaltung […] den Forderungen aus der Einigung bei der Schlichtungsverhandlung vom 14.6.19 beim EDÖB vollumfänglich nachgekommen [ist] und […] die Nachfragen des Antragstellers vom 18.10.19 entsprechend beantwortet [hat]."

E. 15

Gemäss Art. 6 Abs. 1 BGÖ hat jede Person das Recht, amtliche Dokumente einzusehen. Das Öffentlichkeitsgesetz stellt damit eine Vermutung des freien Zugangs zu amtlichen Dokumenten auf. Die Beweislast zur Widerlegung dieser Vermutung obliegt der Behörde, wobei diese hinreichend konkret darzulegen hat, dass bzw. inwiefern eine oder mehrere der gesetzlich vorgesehenen Ausnahmebestimmungen erfüllt sind. Misslingt ihr der Beweis, ist der Zugang grundsätzlich zu gewähren.4

E. 16

Das Öffentlichkeitsgesetz schliesst die erneute Einreichung eines bereits behandelten Zugangsgesuchs nicht aus. Mit anderen Worten ist eine wiederholte Gesucheinreichung durch die gleiche Person grundsätzlich zulässig und an sich nicht bereits rechtsmissbräuchlich.

2 Botschaft zum Bundesgesetz über die Öffentlichkeit der Verwaltung (Öffentlichkeitsgesetz, BGÖ) vom 12. Februar 2003, BBl 2003 2024. 3 GUY-ECABERT, in: Brunner/Mader [Hrsg.], Stämpflis Handkommentar zum BGÖ, Bern 2008 (zit. Handkommentar BGÖ), Art. 13, Rz 8. 4 BVGer Urteil A-1732/2018 vom 26. März 2019, E. 8.

Gemäss Botschaft ist ein Gesuch nur dann missbräuchlich, wenn der Zugangsgesuchsteller zum wiederholten Mal und in systematischer Weise bei der Behörde Zugang zu einem Dokument verlangt, zu welchem ihm – auf Grund dieses Gesetzes oder auf anderem Wege – bereits Zugang gewährt wurde.5 Auch wenn sich vorliegend die Parteien als Schlichtungsergebnis auf die Erstellung eines Berichtes durch das Amt geeinigt haben, bleibt es dem Antragsteller somit grundsätzlich unbenommen, erneut ein inhaltsgleiches Zugangsgesuch einzureichen, wenn er nach Kenntnisnahme des Berichtes weiterhin an den ursprünglich gewünschten Informationen interessiert ist. Dieses Zugangsgesuch muss vom ISB wie jedes andere behandelt werden, zumal ein gleichlautendes Gesuch jederzeit auch von einem anderen Gesuchsteller hätte eingereicht werden können.

E. 17

Das ISB führt in seiner ergänzenden Stellungnahme vom 23. März 2020 an den Beauftragten aus, dass "[d]ie fünf Berichte, die der Bundesrat zur Kenntnis genommen hat, […] als vertraulich klassifiziert [wurden]. Gemäss Art. 6 Abs. 1 der Informationsschutzverordnung (ISchV; SR 510.411) werden Informationen als vertraulich klassifiziert, deren Kenntnisnahme durch Unberechtigte den Landesinteressen Schaden zufügen kann. Die vertrauliche Klassifizierung der fünf Berichte ist heute noch gerechtfertigt, weil er Sicherheitsmassnahmen und –lücken sowie generell Informationen enthält, die Rückschlüsse auf das Sicherheitsdispositiv des Bundes zulassen. Die enthaltenen Informationen können also für Angriffe gegen den Bund missbraucht werden."

E. 18

Demgegenüber bringt der Antragsteller in seiner Stellungnahme vom 20. März 2020 an den Beauftragten vor, dass "die Klassifizierung als «vertraulich» […] nicht für die Verweigerung des Zugangs [genügt], wie in der Botschaft zum BGÖ (ebd.) klar festgehalten ist. Explizit wird dort auch erwähnt, dass insbesondere zu berücksichtigen ist, wie viel Zeit seit der Erstellung bzw. der Klassifizierung des Dokuments vergangen ist."

E. 19

Bei der Beurteilung eines Gesuchs stellt ein Klassifizierungsvermerk lediglich ein Indiz dar, alleine aufgrund der Klassifizierung darf der Zugang jedoch nicht verweigert werden. Unabhängig von einem solchen Vermerk hat die zuständige Stelle von Fall zu Fall überprüfen, ob der Zugang nach Öffentlichkeitsgesetz zu gewähren, zu beschränken, aufzuschieben oder zu verweigern ist (Art. 13 Abs. 3 ISchV). Aus der Koordination der einschlägigen Bestimmungen des Öffentlichkeitsgesetzes und der ISchV ergibt sich, dass die Klassifizierung eines Dokuments oder einer Information nur dann gerechtfertigt ist, wenn eine Ausnahme im Sinne von Art. 7 BGÖ vorliegt.6 Daher muss die Behörde zunächst nachweisen, dass einer der im Öffentlichkeitsgesetz vorgesehenen Ausnahmegründe erfüllt ist, bevor sie den Zugang mit der Begründung einschränken kann, dass das amtliche Dokument klassifiziert ist. Ergibt die Prüfung, dass die Klassifizierung nicht mehr gerechtfertigt ist, ist das Dokument (als Ganzes oder in Anwendung des Verhältnismässigkeitsprinzips in Teilen) zu entklassifizieren und der Zugang muss gewährt werden (Art. 11 Abs. 5 VBGÖ).7 Nachfolgend ist daher zu prüfen, ob die Voraussetzungen für die Anwendung mindestens einer der Ausnahmen des Öffentlichkeitsgesetzes erfüllt sind.

E. 20

Das ISB hielt in seiner Stellungnahme vom 20. Januar 2020 an den Antragsteller fest, dass "die [in den Berichten] aufgeführten Detail-Informationen über Sicherheitslücken oder Schutzmassnahmen […] einem potentiellen Angreifer direkt in die Hand spielen und die gesamte Informatik der Bundesverwaltung sowie von bundesnahen Betrieben gefährden

5 BBl 2003 2017. 6 Bundesamt für Justiz/ Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter, Umsetzung des Öffentlichkeitsprinzips in der Bundesverwaltung: Häufig gestellte Fragen, 7 August 2013, Ziffer 4.2.3; BVGE 2014/24, E. 3.6.3.; Empfehlung vom 5. Februar 2014: NDB/ Statistische Angaben aus Rechenschaftsberichten und aktuelle Zahlen zur ISIS-Datenbank. 7 Empfehlung vom 19. September 2019: EFK/ Prüfungsbericht Gewinnmarge RUAG Aviation, E. 19.

[können]. Der Zugang zu den Berichten muss deshalb wegen Gefährdung der inneren und äusseren Sicherheit der Schweiz (Art. 7 Abs. 1 Bst. c BGÖ) verweigert werden."

E. 21

Diesen Ausführungen hält der Antragsteller in seiner Stellungnahme vom 20. März 2020 an den Beauftragten entgegen, dass "[g]erade in einem Bereich wie der Cybersicherheit, bei der die technische Entwicklung rasant verläuft, […] sich deshalb die Frage [stellt], wie mehrere Jahre alte Sicherheitslücken noch eine Gefährdung für die «gesamte Informatik der Bundesverwaltung sowie von bundesnahen Betrieben», wie es in der Begründung des ISB heisst, darstellen können. Sollten diese Sicherheitslücken auch Jahre später nicht geschlossen sein, wäre dies ein eklatanter Missstand, an dem wiederum ein öffentliches

Interesse besteht. Deshalb ist Punkt 1 der Begründung für die Ablehnung meines Gesuchs mindestens für die Berichte der Jahre 2014, 2015, 2016 und 2017, deren beschriebenen Ereignisse über zwei Jahre zurückliegen, nicht verhältnismässig. […] Zum anderen ist der Grundsatz «Security through obscurity», also dass Sicherheit durch die Geheimhaltung der Funktionsweise geschaffen wird, in der Informatikbranche höchst umstritten bzw. es wird bereits seit Jahren davon abgeraten. Insofern dürften sich die tatsächlich schützenswerten technischen Informationen in den neueren Berichten auf eine überschaubare Zahl beschränken."

E. 22

Nach Art. 7 Abs. 1 Bst. c BGÖ ist der Zugang zu amtlichen Dokumenten einzuschränken, aufzuschieben oder zu verweigern, wenn durch seine Gewährung die innere oder äussere Sicherheit der Schweiz gefährdet werden kann. Nach der Botschaft betrifft diese Ausnahmebestimmungen in erster Linie die Tätigkeit des Polizei-, Zoll-, Nachrichten- und Militärwesens und bezweckt die Geheimhaltung von Massnahmen zum Erhalt der Handlungsfähigkeit der Regierung in ausserordentlichen Lagen, zur Sicherstellung der wirtschaftlichen Landesversorgung, Informationen über technische Einzelheiten oder den Unterhalt von Rüstungsgütern oder Informationen, deren Zugänglichmachung zu einer Beeinträchtigung der Sicherheit wichtiger Infrastrukturen oder gefährdeter Personen führen würde.8 Unabhängig davon wie legitim die Sicherheitszwecke auch sind, sie rechtfertigen es nicht in jedem Fall, alles und jedes geheim zu halten. Auch in diesem Bereich muss stets sorgfältig geprüft werden, ob die Offenlegung der verlangten Informationen die öffentliche Sicherheit tatsächlich ernsthaft gefährden könnte. Auch der Faktor Zeit ist dabei u.a. zu berücksichtigen, kann es doch stark von den Umständen des jeweiligen Zeitpunkts abhängen, insbesondere von der Intensität der Bedrohung für die Bevölkerung, ob eine Information zugänglich gemacht werden kann oder nicht.9

E. 23

Der Zugang darf nicht einfach verweigert werden, wenn ein verlangtes Dokument Informationen enthält, die nach dem Ausnahmekatalog von Art. 7 BGÖ nicht zugänglich sind. Vielmehr ist in diesem Fall das Verhältnismässigkeitsprinzip zu beachten. Bezogen auf das Öffentlichkeitsprinzip bedeutet dies, dass eine Behörde bei Vorliegen einer gerechtfertigten Einschränkung des Zugangs zu einem Dokument hierfür die mildeste, das Öffentlichkeitsprinzip am wenigsten beeinträchtigende Form zu wählen hat. In einer Güterabwägung muss sie prüfen, ob anstelle einer vollständigen Verweigerung ein eingeschränkter, das heisst teilweiser Zugang zu jenen Informationen im Dokument gewährt werden kann, welche nicht geheim zu halten sind, etwa durch Anonymisierung, Einschwärzen, Teilveröffentlichung oder zeitlichen Aufschub."10

8 BBl 2003 2009 f; Empfehlung vom 27. Januar 2017: EFK/ Prüfberichte fedpol, E. 12. 9 COTTIER in: Brunner/Mader [Hrsg.], Stämpflis Handkommentar zum BGÖ, Bern 2008 (zit. Handkommentar BGÖ), Art. 7, Rz.

E. 28

Entsprechend Art. 8 Abs. 2 BGÖ dürfen amtliche Dokument erst zugänglich gemacht werden, wenn der politische oder administrative Entscheid, für den sie die Grundlage darstellen, getroffen ist. Die Bestimmung bezweckt, dass sich die Behörde ihre Meinung frei bilden kann. Besteht jedoch keine Gefahr der Beeinflussung durch die öffentliche Debatte mehr und ist der Entscheid gefällt, ist das Dokument offenzulegen. Damit das

betreffende Dokument als Entscheidungsgrundlage gilt, muss dieses einen direkten und unmittelbaren Zusammenhang mit einem konkreten Entscheid aufweisen und zugleich für diesen von beträchtlichem materiellem Gewicht sein.13 Zudem verlangt der Beauftragte eine gewisse zeitliche Nähe zwischen dem ausstehenden behördlichen Entscheid und dem Zugangsverfahren. Art. 8 Abs. 2 BGÖ sieht lediglich eine befristete Verweigerung, d.h. einen Aufschub des Zugangs vor. Sobald der fragliche Entscheid getroffen ist, muss die Behörde, wenn dannzumal kein Anwendungsfall von Art. 7ff. BGÖ gegeben ist, den Zugang gewähren.14

11 BVGer Urteil A-3829/2015 vom 26. November 2015, E. 7.1.1; BVGer Urteil A-6475/2017 vom 6. August 2018, E. 3.2.2; COTTIER, in: Handkommentar BGÖ, Art. 7, Rz. 27; BBl 2003 1978. 12 Empfehlung vom 27. Januar 2017: EFK/ Prüfberichte fedpol, E. 13; BVGer Urteil A-746/2016 vom 25. August 2016, E. 4.2. 13 BVGer Urteil A-6291/2013 vom 28. Oktober 2014, E.7.1.3. 14 COTTIER, in: Handkommentar BGÖ, Art. 8, Rz. 32f.

E. 29

Vorweg gilt es festzuhalten, dass der Antragsteller Zugang zu Übersichten 2014-2019 verlangt, nicht aber zum Bericht «Informatiksicherheit Bund 2019», der sich nach Aussagen des ISB noch in Vorbereitung befindet. Es ist davon auszugehen, dass die vom Antragsteller gewünschten Informationen zumindest in Teilen bereits vor Erstellung des Berichts 2019 vorhanden sind. Welche dieser Informationen Eingang in den Bericht 2019 zuhanden des Bundesrates finden werden und ob diese Informationen tatsächlich von derart beträchtlichem materiellem Gewicht sind, um einen Entscheid des Bundesrates direkt zu beeinflussen, mithin der Anwendungsfall von Art. 8 Abs. 2 BGÖ gegeben ist15, kann der Beauftragte nicht beurteilen, da er im Schlichtungsverfahren weder im Besitz eines Vorentwurfs des Berichts 2019 noch der relevanten Informationen für die Übersichten ist.

E. 30

Mit dem blossen Verweis auf den noch dem Bundesrat zu unterbreitenden Bericht «Informatiksicherheit Bund 2019» hat das ISB in Bezug auf die verlangten Übersichten 2014- 2019 weder den Zugangsaufschub gemäss Art. 8 Abs. 2 BGÖ noch die vollständige Zugangsverweigerung gestützt auf eine andere Ausnahmebestimmung des Öffentlichkeitsgesetzes hinreichend dargelegt. Damit gilt die Vermutung des Zugangs gemäss Art. 6 BGÖ und das ISB muss entsprechend dem Gesuch Zugang zu den Übersichten 2014-2019 unter Berücksichtigung der Vorgaben des Öffentlichkeitsgesetzes gewähren, soweit die gewünschten Informationen nicht bereits in den Berichten 2014-2018 enthalten sind. III. Aufgrund dieser Erwägungen empfiehlt der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte:

E. 31

Das Informatiksteuerungsorgan des Bundes gewährt einen teilweisen Zugang zu den Berichten "Informatiksicherheit Bund" für die Jahre 2014-2018 unter Berücksichtigung des Verhältnismässigkeitsprinzips und des Zeitablaufs.

E. 32

Das Informatiksteuerungsorgan des Bundes gewährt den Zugang zu den Übersichten für die Jahre 2014-2019 unter Berücksichtigung des Verhältnismässigkeitsprinzips und des Zeitablaufs, soweit die gewünschten Informationen nicht bereits in den Berichten

2014-2018 enthalten sind.

E. 33

Der Antragsteller kann innerhalb von 10 Tagen nach Erhalt dieser Empfehlung beim Informatiksteuerungsorgan des Bundes den Erlass einer Verfügung nach Art. 5 des Bundesgesetzes über das Verwaltungsverfahren (Verwaltungsverfahrensgesetz, VwVG; SR 172.021) verlangen, wenn er mit der Empfehlung nicht einverstanden ist (Art. 15 Abs. 1 BGÖ).

E. 34

Das Informatiksteuerungsorgan des Bundes erlässt eine Verfügung, wenn sie mit der Empfehlung nicht einverstanden ist (Art. 15 Abs. 2 BGÖ).

E. 35

Das Informatiksteuerungsorgan des Bundes erlässt die Verfügung innert 20 Tagen nach Empfang dieser Empfehlung oder nach Eingang eines Gesuches um Erlass einer Verfügung (Art. 15 Abs. 3 BGÖ).

E. 36

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

15 BVGer Urteil A-2070/2017 vom 16. Mai 2018, E. 4.4.2.

8/8

E. 37

Die Empfehlung wird eröffnet: - Einschreiben mit Rückschein (R) X

- Einschreiben mit Rückschein (R) Informatiksteuerungsorgan des Bundes Schwarztorstrasse 59 3003 Bern

Reto Ammann