EDOEB empfehlung-vom-28-maerz-2023-bj-upreg-datenbankauszuggefaehrdung-der-inneren-ode-2023-03-28 vom 28. März 2023

EDÖB, 2023-03-28, DE

Quelle: https://mcp.opencaselaw.ch/entscheid/edoeb_empfehlung-vom-28-maerz-2023-bj-upreg-datenbankauszuggefaehrdung-der-inneren-ode-2023-03-28

FR: EDOEB empfehlung-vom-28-maerz-2023-bj-upreg-datenbankauszuggefaehrdung-der-inneren-ode-2023-03-28 du 28 mars 2023

IT: EDOEB empfehlung-vom-28-maerz-2023-bj-upreg-datenbankauszuggefaehrdung-der-inneren-ode-2023-03-28 del 28 marzo 2023

Erwägungen

E. 1

Schlusstitel des Schweizerischen Zivilgesetzbuches (SchlT ZGB; SR 210).

E. 2

s.a. Elektronische öffentliche Urkunden und elektronische Beglaubigungen (admin.ch), besucht am 22. März 2023.

E. 3

Im UPReg werden die Urkundspersonen gemäss Art. 7 EÖBV mit den folgenden Daten eingetra- gen: a. die Namen und Vornamen gemäss Pass oder Identitätskarte; b. Geburtsdatum; c. Staatsangehörigkeit; d. Berufs- oder Funktionsbezeichnung nach dem massgebenden Recht sowie Bezeichnung des massgebenden Kantons oder der Bundesbehörde; e. Unternehmens-Identifikationsnummer (UID) nach dem Bundesgesetz über die Unterneh- mens-Identifikationsnummer (UIDG; SR 431.03) und gegebenenfalls im massgebenden Kanton verwendete Nummer der Urkundsperson; f. Geschäfts- oder Amtsadresse gemäss Eintrag im UID-Register (Art. 6 UIDG); g. Datum der Erteilung der amtlichen Befugnis; h. gegebenenfalls Datum des Wegfalls der amtlichen Befugnis; i. zur Überprüfung von Signaturen und zur Authentifizierung der Urkundsperson durch das UP-Reg: 1. falls dauerhafte Zertifikate verwendet wurden oder werden: diese Zertifikate, 2. falls Einmalzertifikate verwendet wurden oder werden: die dauerhaften Seriennummern oder andere Elemente dieser Zertifikate, die eine eindeutige Identifikation der Urkundsperson ermöglichen, sowie Angaben über den verwendeten Authentifizierungs-Mechanismus. Das UPReg macht diese Daten mit Ausnahme des Geburtsdatums und der Staatsangehörigkeit der Urkundsperson im Internet öffentlich zugänglich (Art. 5 Abs. 1 und Art 9 Bst. a e contra- rio EÖBV).

E. 4

Die Antragstellerin (Privatperson) hat am 9. September 2022 gestützt auf das Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz, BGÖ; SR 152.3) beim BJ um Ein- sicht ersucht in "das Dokument bzw. UPREG-Datenbankauszug: Bezogene Funktionsnach- weise/Zulassungsbestätigungen im Jahr 2021 mit mindestens den Feldern IP-Nummer, UID- Nummer Notar, Datum, Zeitpunkt (Zeitstempel)."

E. 5

Am 20. September 2022 nahm das BJ Stellung zum Zugangsgesuch und erklärte, dass der von der Antragstellerin verlangte Auszug Informationen beinhalte, mit welchen offengelegt würde, wann und wie häufig Notarinnen und Notare elektronische Ausfertigungen oder elektronische Ko- pien erstellt haben. Diese Daten würden in die Privatsphäre Dritter fallen. Ein überwiegendes öf- fentliches Interesse, welches die Einsichtnahme trotzdem rechtfertigen würde, sei nicht ersichtlich und sei auch von der Antragstellerin nicht dargetan worden.

E. 6

Mit Schreiben vom 23. September 2022 reichte die Antragstellerin einen Schlichtungsantrag beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (Beauftragter) ein.

E. 7

Mit E-Mail vom 28. September 2022 bestätigte der Beauftragte gegenüber der Antragstellerin den Eingang des Schlichtungsantrages und forderte gleichentags das BJ dazu auf, die betroffenen Dokumente sowie bei Bedarf eine ergänzende Stellungnahme einzureichen.

E. 8

Mit E-Mail 12. Oktober 2022 reichte das BJ dem Beauftragten einen Screenshot eines Beispiels eines Auszugs mit den verlangten Informationen ein. Dazu erklärte es, die IP-Adresse (Internet Protocol-Adresse) sei in einer (separaten) Logdatei gespeichert. Sie diene daher lediglich der si- cherheitstechnischen Prüfung, nicht jedoch der Identifikation und Authentisierung der Urkunds- person, weil sie dazu nicht geeignet sei. Auf eine weitergehende Stellungnahme verzichtete das BJ.

E. 9

Am 16. Februar 2023 fand eine Schlichtungsverhandlung statt, in welcher sich die Parteien nicht einigen konnten.

E. 10

Mit E-Mail vom 27. Februar 2023 an den Beauftragten berief sich das BJ für seine Zugangsver- weigerung auf Art. 7 Abs. 1 Bst. g BGÖ (Offenlegung von Berufs- und Geschäftsgeheimnissen) sowie Art. 7 Abs. 2 BGÖ (Schutz der Privatsphäre) und argumentierte, dass ein Vergleich zur analogen Welt der Beurkundung (kantonale Urkundenregister) zeige, dass es einer gesuchstel- lenden Person nicht möglich sei, die Anzahl ausgestellter physischer Urkunden pro Notar zu er- fragen. Es sei nicht ersichtlich, weshalb die Einsicht in der digitalen Welt zugänglich sein sollte, zumal das UPReg das Ziel habe, die analoge Welt in digitaler Form nachzubilden. Die Herausgabe sämtlicher IP-Adressen könne sicherheitstechnische Probleme verursachen. So könnte in unzu- lässiger Weise auf das UPReg eingewirkt werden, etwa durch IP-Address-Spoofing.4 Ausserdem lasse eine Auflistung der IP-Adressen den Rückschluss zu, wo sich das Gerät, das einer registrier- ten Person spezifisch zugeordnet sei, im Moment befinde. Insofern sei eine Einsichtnahme auf- grund von Art. 7 Abs. 1 Bst. c BGÖ zu verweigern.

E. 11

Mit E-Mail vom 28. Februar 2023 erklärte die Antragstellerin dem Beauftragten, es sei unmöglich, anhand der Anzahl der abgerufenen Funktionsnachweise (FN) bzw. Zulassungsbestätigungen auf den Umsatz oder die Anzahl der bearbeiteten Fälle eines Notars zu schliessen. Es treffe nicht zu, dass der Zeitpunkt des Anbringens eines Funktionsnachweises dazu führen könne, dass in klei- nen Gemeinden Klienten eines Notars erkannt würden und Rückschlüsse auf die Klientschaft ge- zogen werden könne. Diese würden nach wie vor zum Notar zur analogen Beurkundung gehen. "Wenn der Notar einen FN abruft, hat er in diesem Moment eine quasi hoheitliche Funktion, indem er stellvertretend für den Staat und die Öffentlichkeit eine öffentliche Beurkundung durchführt. Die verlangten Logdaten bilden ausschliesslich diese Sekunden ab, in denen die Software Cygillum (oder die Terravis-Plattform) den Abgleich mit dem UPReg ausführt. Die ausgeführten IP-Adres- sen zeigen die von den [Notaren und Notarinnen] verwendete Adressen. Allerdings ist es nicht erforderlich, dass diese IP-Adressen fix sind und die IP-Adressen werden beim Anmeldeprozess nicht im UPReg hinterlegt, sind mithin also kein Bestandteil des Login- oder Abfrageprozesses für FN."

E. 12

Auf die weiteren Ausführungen der Antragstellerin und des BJ sowie auf die eingereichten Unter- lagen 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. 13

Die Antragstellerin reichte beim BJ ein Zugangsgesuch nach Art. 10 BGÖ ein. Dieses verweigerte den Zugang zu den verlangten Dokumenten. Die Antragstellerin ist als Teilnehmerin 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 Beauf- tragten eingereicht (Art. 13 Abs. 2 BGÖ).

E. 14

Das Schlichtungsverfahren findet auf schriftlichem Weg oder konferenziell (mit einzelnen oder allen Beteiligten) unter Leitung des Beauftragten statt, der das Verfahren im Detail festlegt.5 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.

4 https://de.wikipedia.org/wiki/IP-Spoofing), besucht am 22. März 2023. 5 Botschaft zum Bundesgesetz über die Öffentlichkeit der Verwaltung (Öffentlichkeitsgesetz, BGÖ) vom 12. Februar 2003, BBl 2003 1963 (zitiert BBl 2003), BBl 2003 2024.

 B. Materielle Erwägungen

E. 15

Der Beauftragte prüft nach Art. 12 Abs. 1 der Verordnung über das Öffentlichkeitsprinzip der Ver- waltung (Öffentlichkeitsverordnung, VBGÖ; SR 152.31) die Rechtmässigkeit und die Angemes- senheit der Beurteilung des Zugangsgesuches durch die Behörde.6

E. 16

Vorweg ist zu bemerken, dass jede Person das Recht hat, amtliche Dokumente einzusehen und von den Behörden Auskunft über den Inhalt amtlicher Dokumente zu erhalten (Art. 6 Abs. 1 BGÖ). Damit wird jeder Person ein generelles Recht auf Zugang zu amtlichen Dokumenten, über welche die Verwaltung verfügt, gewährt, ohne dass ein besonderes Interesse nachgewiesen werden muss.7 Daher muss die Antragstellerin kein überwiegendes öffentliches Interesse in ihrem Zu- gangsgesuch dartun (Ziffer 5).

E. 17

Die Antragstellerin verlangt Zugang zu den UID-Nummern der Notarinnen und Notare für das Jahr 2021. Die verlangten UID-Nummern sind ebenso wie die Namen der Urkundspersonen im UPReg öffentlich abrufbar (Art. 7 Bst. e EÖBV). Im UPReg kann, soweit für den Beauftragten ersichtlich, jedoch keine Selektion für das Jahr 2021 vorgenommen werden. Für dieses Jahr hat das BJ weder vorgebracht, dass diese Informationen nicht mit einem einfachen elektronischen Vorgang herge- stellt werden können (Art. 5 Abs. 2 BGÖ e contrario), noch hat es sich auf Art. 6 Abs. 3 BGÖ berufen. Somit ist das BJ der objektiven Beweislast zur Widerlegung der Vermutung des freien Zugangs nicht gebührend nachgekommen, weshalb der Zugang grundsätzlich zu gewähren ist.8

E. 18

Zwischenfazit: Für die im Jahr 2021 eingetragenen Urkundspersonen (Notariat) ist der Zugang zu den UID-Nummern zu gewähren.

E. 19

Nicht öffentlich zugänglich sind hingegen die Funktionsnachweise/Zulassungsbestätigungen, die IP-Adresse, Datum, Zeitpunkt (Zeitstempel), welche die Antragstellerin für das Jahr 2021 verlangt hat.

E. 20

Das BJ bezieht sich hinsichtlich der Zugangsverweigerung zu den IP-Adressen auf die Ausnah- menorm von Art. 7 Abs. 1 Bst. c BGÖ und führt aus: "Die Herausgabe der IP-Adressen könnte zudem sicherheitstechnische Probleme verursachen. Denn: wer die sichere IP-Adressen kennt, könnte diese verwenden bzw. Dritten zur Verfügung stellen. Mit diesen IP-Adressen könnte in unzulässiger Weise auf das UPREG eingewirkt werden, etwa durch IP-Address-Spoofing, vgl. etwa https://de.wikipedia.org/wiki/IP-Spoofing). Ausserdem lässt eine Auflistung der IP-Adressen den Rückschluss zu, wo sich das Gerät, das einer registrierten Person spezifisch zugeordnet ist, im Moment der Benutzung befindet."

E. 21

Die Antragstellerin wendet ein, dass ein Notar, der einen Funktionsnachweis abrufe, in dem Mo- ment eine quasi hoheitliche Funktion ausübe, indem er stellvertretend für den Staat und die Öf- fentlichkeit eine öffentliche Beurkundung durchführe. Die verlangten Logdaten würden ausschliesslich die Sekunden abbilden, in denen die Software Cygillum (oder die Terravis-Platt- form) den Abgleich mit dem UPReg ausführe. Die aufgeführten IP-Adressen würden zwar die von den Notarinnen und Notaren verwendeten IP-Adressen zeigen. Allerdings sei es nicht erforderlich, dass diese IP-Adressen fix seien. Die IP-Adressen würden beim Anmeldeprozedere nicht im UP- Reg hinterlegt, mithin seien diese also kein Bestandteil des Login- oder Abfrageprozesses für Funktionsnachweise.

E. 22

Nach Art. 7 Abs. 1 Bst. c BGÖ kann der Zugang zu amtlichen Dokumenten eingeschränkt, aufge- schoben oder verweigert werden, wenn durch seine Gewährung die innere oder äussere Sicher- heit der Schweiz gefährdet werden kann. Gemäss der Botschaft zum Öffentlichkeitsgesetz9 betrifft diese Ausnahmebestimmung in erster Linie die Tätigkeit des Polizei-, Zoll-, Nachrichten- und Mi- litärwesens und bezweckt die Geheimhaltung von Massnahmen zum Erhalt der Handlungsfähig- keit der Regierung in ausserordentlichen Lagen, zur Sicherstellung der wirtschaftlichen

6 GUY-ECABERT, in: Brunner/Mader [Hrsg.], Stämpflis Handkommentar zum BGÖ, Bern 2008 (zit. Handkommentar BGÖ), Art. 13, Rz 8. 7 Urteil des BVGer A-4494/2020 vom 20. April 2021 E. 4.2.2. 8 Urteil des BVGer A-4494/2020 vom 20. April 2021 E. 4.2.2. 9 BBl 2003 2009.

5/9 Landesversorgung, Informationen über technische Einzelheiten oder den Unterhalt von Rüstungs- gütern oder Informationen, deren Zugänglichmachung zu einer Beeinträchtigung der Sicherheit wichtiger Infrastrukturen oder gefährdeter Personen führen würde. Dabei ist nach der Rechtspre- chung10 nicht die Abgrenzung nach den tätigen Behörden massgeblich, sondern die Abgrenzung von gefährdeten Interessen und Rechtsgütern. Sicherheit ist hierbei sowohl als Unverletzlichkeit der Rechtsgüter der Einzelnen wie auch des Staates und seiner Einrichtungen sowie der Rechts- ordnung insgesamt zu verstehen. Die innere und äussere Sicherheit der Schweiz kann durch An- griffe und Bedrohungen wie Kriminalität im Allgemeinen, Extremismus und Terrorismus sowie militärische und nachrichtendienstliche Aktivitäten gefährdet sein. Von der Bestimmung erfasst wird ebenfalls der Schutz von sicherheitsrelevanten Informationen im Zusammenhang mit kriti- schen Infrastrukturen der Landesversorgung wie informations-, kommunikations- und energie- technischen Einrichtungen. Allerdings muss nach der Rechtsprechung selbst bei legitimen Sicherheitszwecken sorgfältig geprüft werden, ob die Offenlegung der verlangten Dokumente die öffentliche Sicherheit ernsthaft gefährden könnte. Als Leitlinie der Prüfung dient dabei das Krite- rium, wie weit es verantwortbar ist, dass über die Bekanntgabe von Informationen, die danach auch der gesamten Öffentlichkeit offen stünden, Zugang zu Wissen besteht, das sich in uner- wünschter bzw. für die innere Sicherheit der Schweiz nachteiliger Weise nutzen liesse.

E. 23

Bei den IP-Adressen handelt es sich um Adressierungselemente im Sinne der Fernmeldegesetz- gebung.11 Es sind numerische Kommunikationsparameter, welche die Identifikation einer insbe- sondere aus Netzrechnern oder -servern bestehenden Internet-Domain sowie der Benutzerrechner, die an den Verbindungen in diesem Netz beteiligt sind, ermöglichen. Mit ande- ren Worten wird durch die IP-Adresse jeder an das Internet angeschlossene Computer identifi- ziert. Immer wenn im Internet Daten abgefragt werden, so zum Beispiel beim Aufrufen einer Website, übermittelt der Computer des Benutzers seine Anfrage verbunden mit der ihm zugewie- senen IP-Adresse. Wird einem Rechner eine IP-Adresse fest zugewiesen, spricht man von einer statischen IP-Adresse. Verbindet sich ein Benutzer über einen Internet-Dienstanbieter (Provider) mit dem Internet, erhält er jedoch meist eine dynamische IP-Adresse, das heisst, seinem Compu- ter/Router wird bei jeder Verbindungsaufnahme neu irgendeine freie Adresse aus dem Pool des Providers zugewiesen. Da die Router ständig mit dem Internet verbunden sind, ändert sich die vom System zugewiesene IP-Adresse nur sporadisch. Da bedeutet, dass eine

Identifikation des betreffenden Rechners/Routers durch diese IP-Adresse auch über den einzelnen Nutzungsvor- gangs hinaus möglich ist. Ob eine Information aufgrund zusätzlicher Angaben mit einer Person in Verbindung gebracht werden kann, sich die Information mithin auf eine bestimmbare Person be- zieht (Art. 3 Bst. a DSG12), beurteilt sich gemäss Bundesgericht13 aus der Sicht des jeweiligen Inhabers der Information.

E. 24

Nach Art. 57l des Regierungs- und Verwaltungsorganisationsgesetzes (RVOG; SR 172.010) dür- fen Bundesorgane Personendaten, die bei der Nutzung der elektronischen Infrastruktur anfallen, aufzeichnen, so gemäss Bst. b die Daten über die Nutzung der elektronischen Infrastruktur: 1. zur Aufrechterhaltung der Informations- und Dienstleistungssicherheit, 2. zur technischen Wartung der elektronischen Infrastruktur, 3. zur Kontrolle der Einhaltung von Nutzungsreglementen, 4. zum Nachvollzug des Zugriffs auf Datensammlungen, 5. zur Erfassung der Kosten, die durch die Benutzung der elektronischen Infrastruktur entstehen. Das BJ speichert die IP-Adresse in einer (separaten) Logdatei (Ziffer 8). Laut BJ kann die Her- ausgabe der IP-Adressen sicherheitstechnische Probleme verursachen. So könne in unzulässiger Weise auf das UPReg eingewirkt werden, etwa durch IP-Address-Spoofing (s. Ziffer 10 und 20). Diese Begründung des BJ ist für den Beauftragte plausibel. Es ist bekannt, dass die Kenntnis einer IP-Adresse (Internetworking Protocol Address) eine potentielle Bedrohung für den Zugang zu Computersystemen ist. So kann sich eine nicht zugangsberechtigte als zugangsberechtigte

10 Urteil des BVGer A-407/2019 vom 14. Mai 2020 E. 5.1 m.w.H. 11 s.a. Fernmeldegesetz (FMG; SR 784.10). 12 Bundesgesetz über den Datenschutz (DSG; SR 235.1). 13 s.a. BGE 136 II 508 E. 3.3 f.

6/9 Person ausgeben und vortäuschen, ihre Kommunikation stamme von einer dem System vertrau- ten Person. Durch diese Täuschung kann ein Sicherheitssystem umgangen werden. So erhöht die Offenlegung der IP-Adressen die Wahrscheinlichkeit und das Risiko, dass die UPReg Daten- bank Cyberangriffen ausgesetzt werden könnte. Damit ist nach Ansicht des Beauftragten erstellt, dass die Bekanntgabe von IP-Adressen, die danach auch der gesamten Öffentlichkeit offen stün- den, Zugang zu Wissen besteht, das sich in unerwünschter bzw. für die innere Sicherheit der Schweiz nachteiliger Weise nutzen liesse.

E. 25

Zwischenfazit: In Bezug auf die IP-Adresse ist nach Ansicht des Beauftragten das Vorliegen des Ausnahmetatbestandes von Art. 7 Abs. 1 Bst. c BGÖ als erfüllt zu betrachten.

E. 26

Mit diesem Resultat erübrigt sich die Prüfung der Vorbringen des BJ, ob mit der Offenlegung der IP-Adresse die Privatsphäre nach Art. 7 Abs. 2 BGÖ beeinträchtigt ist.

E. 27

Die Schweiz kennt drei verschiedene Notariatssysteme: Das freie Notariat, das von einem freibe- ruflichen Notar mit kantonaler Zulassung ausgeübt wird, das Amtsnotariat, welches von einem vom Staat angestellten Beamten oder Funktionär erfüllt wird, sowie das gemischte System, das beide Formen im gleichen Kanton zulässt. In einigen Kantonen können auch andere Funktions- träger als Notare gewisse standardisierte Rechtsakte vornehmen, z.B. Handelsregisterführer, Ge- meindeschreiber.14

E. 28

Das BJ erklärt gestützt auf Art. 7 Abs. 1 Bst. g BGÖ und Art. 7 Abs. 2 BGÖ, dass der verlangte Auszug Daten betreffe, die den Abruf von Zulassungsbestätigungen nach Art. 2 Bst. b und Art. 10 Abs. 1 Bst. e EÖBV und damit die Anzahl der verwendeten Urkunden zeige. Die Anzahl würde Rückschlüsse über die Beurkundungstätigkeit zeigen, so z.B. ob und wie oft die elektrische Ur- kunde und in welchen Zeitabständen diese benutzt werde. Damit seien, wenn auch vage, Rück- schlüsse möglich, namentlich zusammen mit Erfahrungswerten über die notarielle Tätigkeit des einzelnen Notars sowie über dessen Einkünfte. Je kleiner die Gemeinde, desto präziser könnten Rückschlüsse gezogen werden, so auch auf einzelne Klienten. So bestehe das Risiko, dass eine bestimmte Person überwacht werde. Der Umstand, dass heute die elektronische öffentliche Be- urkundung möglicherweise zahlenmässig noch nicht oft verwendet werde – und die Log-Files da- mit nicht allzu viele Einträge aufweisen – dürfe kein Kriterium für die Herausgabe sein. Ein Vergleich zur analogen Welt der Beurkundung (kantonale Urkundenregister) zeige, dass es einem Gesuchsteller nicht möglich sei, die Anzahl ausgestellter physischer Urkunden pro Notar zu erfra- gen. Es sei nicht ersichtlich, weshalb die Einsicht in der digitalen Welt zugänglich sein sollte, zumal das UPReg das Ziel habe, die analoge Welt in digitaler Form nachzubilden.

E. 29

Demgegenüber wendet die Antragstellerin ein, es sei unmöglich, anhand der Anzahl abgerufener Funktionsnachweise auf den Umsatz oder die Anzahl der bearbeiteten Fälle eines Notars zu schliessen. Die Anzahl Funktionsnachweise pro Geschäft hänge u.a. von der Anzahl der Beilagen ab, die mit einem Funktionsnachweis zu versehen seien. Auch lasse sich aufgrund der Anzahl Funktionsnachweise nicht auf den Umsatz schliessen. Die Notariatsgebühr bemesse sich nach dem Arbeitsaufwand, nach der Bedeutung des Geschäfts und nach der von der Notarin oder vom Notar übernommenen Verantwortung. Keiner dieser Faktoren könne mit der Anzahl Funktions- nachweise in Verbindung gebracht werden, variiere doch der Umsatz pro Geschäft von einigen hundert Franken bis zu mehreren zehntausend Franken. Es treffe nicht zu, dass der Zeitpunkt der Anbringung eines Funktionsnachweises dazu führen könne, dass in kleinen Gemeinden Klienten eines Notars erkannt und Rückschlüsse auf die Identität bzw. Klientengeschäfte gezogen werden können. Diese Klienten gingen nach wie vor zur analogen Beurkundung zum Notar. Bei diesem Besuch werde die Papier-Urkunde erstellt. Im Nachgang werde irgendwann eine E-Ausfertigung erstellt und es würden alle weiteren Unterlagen für die E-Eingabe bereitgestellt. Im Rahmen dieser nachgelagerten Arbeiten würden der Funktionsnachweis abgerufen. Die Ausfertigung werde so gut wie nie in Präsenz des Klienten erstellt, dessen Präsenz sei dafür auch nicht erforderlich. Wenn der Notar einen Funktionsnachweis abrufe, habe er in diesem Moment eine quasi hoheitli- che Funktion, indem er stellvertretend für den Staat und die Öffentlichkeit eine öffentliche Beur- kundung durchführe. Die verlangten Logdaten würden ausschliesslich diese Sekunden abbilden,

14 Preisüberwacher Kantonale Notariatstarife, Broschüre 2007, besucht am 22. März 2023, S. 1.

7/9 in denen die Software Cygillum (oder die Terravis-Plattform) den Abgleich mit dem UPReg aus- führe.

E. 30

Entsprechend Art. 7 Abs. 1 Bst. g BGÖ kann der Zugang eingeschränkt, aufgeschoben oder ver- weigert werden, wenn durch die Bekanntgabe amtlicher Dokumente Berufs-, Geschäfts- oder Fab- rikationsgeheimnisse offenbart werden können. Der Begriff „Geschäftsgeheimnis“ ist gesetzlich nicht definiert. Nach der bundesgerichtlichen Rechtsprechung wird als Geheimnis jede in Bezie- hung mit dem betroffenen Geheimnisträger stehende Tatsache qualifiziert, welche weder offen- kundig noch allgemein zugänglich ist (relative Unbekanntheit), welche der Geheimnisherr geheim halten will (subjektives Geheimhaltungsinteresse) und an deren Geheimhaltung der Geheimnis- herr ein berechtigtes Interesse hat (objektives Geheimhaltungsinteresse).15

E. 31

Vom Geheimnisbegriff werden jedoch nicht alle Geschäftsinformationen erfasst, sondern nur die wesentlichen Daten, deren Kenntnisnahme durch die Konkurrenz Marktverzerrungen bewirken und dazu führen würde, dass dem betroffenen Unternehmen ein Wettbewerbsvorteil genommen bzw. ein Wettbewerbsnachteil und damit ein Schaden zugefügt wird. Der Gegenstand des Ge- schäftsgeheimnisses muss geschäftlich relevante Informationen betreffen. Darunter können ins- besondere Informationen fallen, die Einkaufs- und Bezugsquellen, Betriebsorganisation, Preiskalkulation, Geschäftsstrategien, Businesspläne sowie Kundenlisten und -beziehungen be- treffen und einen betriebswirtschaftlichen oder kaufmännischen Charakter aufweisen. Entschei- dend ist, ob diese Informationen Auswirkungen auf das Geschäftsergebnis haben können, oder mit anderen Worten, ob diese Informationen bei einer Zugänglichmachung an Dritte Auswirkungen auf die Wettbewerbsfähigkeit der Unternehmung haben. Ein abstraktes Gefährdungsrisiko genügt nicht.16 Die Verletzung des Geschäftsgeheimnisses muss aufgrund der Zugänglichkeit des betref- fenden Dokuments wahrscheinlich erscheinen; eine lediglich denkbare oder (entfernt) mögliche Gefährdung reicht nicht aus. Als Beeinträchtigung kann zudem nicht jede geringfügige oder un- angenehme Konsequenz des Zugangs zum gewünschten amtlichen Dokument wie etwa zusätz- liche Arbeit oder unerwünschte öffentliche Aufmerksamkeit gelten. Die drohende Verletzung muss gewichtig und ernsthaft sein.17

E. 32

Das Argument des BJ, wonach es in der anlogen Welt nicht möglich sei, Zugang zu den kantona- len Registern zu nehmen, ist insofern bedeutsam, als auch diese zeigen, wie viele Beurkundungen eine Notarin oder Notarin vorzuweisen hat. Auch wenn sich bei der Anzahl von Zulassungsbestä- tigungen durch das UPReg nicht genau eruieren lässt, wie hoch der Verdienst der betreffenden Urkundsperson ist, hat diese Zahl durchaus betriebswirtschaftlichen Charakter. Es kann nach An- sicht des Beauftragten nicht ausgeschlossen werden, dass dadurch Rückschlüsse auf die wirt- schaftliche Aktivität einer freischaffenden Notarin oder eines freischaffenden Notars möglich sind, welche im eigenen Namen, auf eigene Rechnung sowie eigenes Risiko handeln. Eine drohende Verletzung des Geschäftsgeheimnisses ist daher nicht auszuschliessen, da die Offenlegung der verlangten Informationen das Ergebnis wirtschaftlicher Vorgänge beeinflussen und einen Wettbe- werbsnachteil zur Folge haben kann. Nach Ansicht des Beauftragten hat das BJ den Ausnahme- tatbestand von Art. 7 Abs. 1 Bst. g BGÖ in Bezug auf die freischaffenden Notarinnen und Notare plausibel dargelegt.

E. 33

Dies gilt ebenso für die privaten Urkundspersonen in Kantonen, die das System amtliche Notare und private Urkundspersonen für Beglaubigungen kennen (Ziffer 27), soweit sie als private Ur- kundsperson im eigenen Namen und auf eigene Rechnung sowie auf eigenes Risiko handelt.

E. 34

Zwischenfazit: Nach Ansicht des Beauftragten ist der vom BJ geltend gemachte Ausnahmegrund nach Art. 7 Abs. 1 Bst. g BGÖ in Bezug auf die verlangten, nicht öffentlich zugänglichen Informa- tionen des UPReg betreffend die freischaffenden und privaten Notarinnen und Notare plausibel dargelegt.

15 Urteil des BGer 1C_665/2017 vom 16. Januar 2019 E. 3.3. 16 Urteil des BGer 1C_665/2017 vom 16. Januar 2019 E. 3.3; Urteil des BVGer A-3367/2017 vom 3. April 2018 E. 7.4. 17 Urteil des BVGer A-199/2018 vom 18. April 2019 E. 3.2.2.

E. 35

Mit diesem Resultat erübrigt sich die Prüfung der Vorbringen des BJ, ob durch die Offenlegung der verlangten Informationen die Privatsphäre der im eigenen Namen und auf eigene Rechnung tätigen Urkundspersonen oder ihrer Kundschaft nach Art. 7 Abs. 2 BGÖ beeinträchtigt ist.

E. 36

Offen ist noch die Prüfung von Ausnahmegründen für das Amtsnotariat. Das BJ hat sich im Schlichtungsverfahren nicht zu dieser spezifischen Kategorie geäussert. Das Vorliegen von Ge- schäftsgeheimnissen ist nach Ansicht des Beauftragten hierbei aber nicht offensichtlich, da Amts- notarinnen und Amtsnotare – im Unterschied zu freischaffenden Urkundspersonen – die Beurkundungen im Namen und Rechnung der Verwaltung und in deren Verantwortung ausführen. Damit hat das BJ nicht mit der von der Rechtsprechung geforderten Begründungsdichte dargelegt, inwiefern die Ausnahmebestimmung nach Art 7 Abs.1 Bst. g BGÖ (Offenlegung von Geschäfts- geheimnissen) sowie nach Art. 7 Abs. 2 BGÖ (Beeinträchtigung der Privatsphäre) für die als Amts- notarinnen und Amtsnotare tätigen Urkundspersonen für das Jahr 2021 erfüllt sind.18 Nach Ansicht des Beauftragten ist diesbezüglich die gesetzliche Vermutung des grundsätzlich freien Zugangs somit nicht widergelegt.

E. 37

Zusammenfassend hält der Beauftragte fest, dass - hinsichtlich der IP-Adresse das Vorliegen des Ausnahmetatbestandes von Art. 7 Abs. 1 Bst. c BGÖ gegeben ist (Ziffer 25); - der Zugang zu den UID-Nummern für die im Jahr 2021 eingetragenen Urkundspersonen (Nota- riat) zu gewähren ist (Ziffer 18); - der Ausnahmetatbestand von Art. 7 Abs. 1 Bst. g BGÖ in Bezug auf die verlangten, nicht öffent- lich zugänglichen Informationen des UPReg für das 2021 hinsichtlich der freischaffenden und privaten Notarinnen und Notare vom BJ plausibel dargetan wurde (Ziffer 34); - der Ausnahmetatbestand nach Art. 7 Abs. 1 Bst. g BGÖ und Art. 7 Abs. 2 BGÖ in Bezug auf die verlangten, nicht öffentlich zugänglichen Informationen des UPReg für das Jahr 2021 hinsichtlich der Amtsnotarinnen und Amtsnotare vom BJ nicht rechtsgenüglich dargetan wurde, weshalb das BJ die gesetzliche Vermutung des grundsätzlich freien Zugangs nicht widerlegen konnte (Ziffer 36). III Aufgrund dieser Erwägungen empfiehlt der Eidgenössische Datenschutz- und Öffentlich-

keitsbeauftragte:

E. 38
Das BJ hält an der Zugangsverweigerung betreffend die IP-Adressen fest.

E. 39
Das BJ gewährt den Zugang zu den UID-Nummern, der im Jahr 2021 im UPReg registrierten freischaffenden und privaten Notarinnen und Notare sowie der Amtsnotarinnen und Amtsnotare.

E. 40
Das BJ hält hinsichtlich der freischaffenden und privaten Notarinnen und Notare an der Zugangs- verweigerung zu allen nicht öffentlich zugänglichen Informationen des UPReg, welche die Antrag- stellerin für das Jahr 2021 verlangt hat, fest.

E. 41
Da BJ gewährt, mit Ausnahme der IP-Adressen, den Zugang zu den von der Antragstellerin ver- langten Informationen hinsichtlich der Amtsnotarinnen und Amtsnotare für das Jahr 2021, da es bisher die gesetzliche Vermutung des Zugangs diesbezüglich nicht widerlegen konnte.

E. 42
Die Antragstellerin kann innerhalb von 10 Tagen nach Erhalt dieser Empfehlung beim BJ den Erlass einer Verfügung nach Art. 5 des Bundesgesetzes über das Verwaltungsverfahren (Verwal- tungsverfahrensgesetz, VwVG; SR 172.021) verlangen, wenn sie mit der Empfehlung nicht ein- verstanden ist (Art. 15 Abs.1 BGÖ).

E. 43
Das BJ erlässt eine Verfügung, wenn es mit der Empfehlung nicht einverstanden ist (Art. 15 Abs. 2 BGÖ).

18 Urteil des BVGer A-4494/2020 vom 20. April 2021 E. 4.2.2.

E. 44
Das BJ erlässt die Verfügung innert 20 Tagen nach Empfang dieser Empfehlung oder nach Ein- gang eines Gesuches um Erlass einer Verfügung (Art. 15 Abs. 3 BGÖ)

E. 45
Diese Empfehlung wird veröffentlicht. Zum Schutz der Personendaten der am Schlichtungsver- fahren Beteiligten wird der Name der Antragstellerin anonymisiert (Art. 13 Abs. 3 VBGÖ).

E. 46
Die Empfehlung wird eröffnet: - Einschreiben mit Rückschein (R) X.___

- Einschreiben mit Rückschein (R) Bundesamt für Justiz BJ 3003 Bern

Reto Ammann

Astrid Schwegler Leiter Direktionsbereich

Juristin Direktionsbereich Öffentlichkeitsprinzip

Öffentlichkeitsprinzip