



Sachstand

**Aufbewahrung behördlicher Messengerkommunikation und ihre
Verwendung als Beweismittel in Deutschland und anderen
europäischen Staaten**

Aufbewahrung behördlicher Messengerkommunikation und ihre Verwendung als Beweismittel in Deutschland und anderen europäischen Staaten

Aktenzeichen: WD 3 - 3000 - 097/24
Abschluss der Arbeit: 29. Oktober 2024
Fachbereich: WD 3: Verfassung und Verwaltung

Die Wissenschaftlichen Dienste des Deutschen Bundestages unterstützen die Mitglieder des Deutschen Bundestages bei ihrer mandatsbezogenen Tätigkeit. Ihre Arbeiten geben nicht die Auffassung des Deutschen Bundestages, eines seiner Organe oder der Bundestagsverwaltung wieder. Vielmehr liegen sie in der fachlichen Verantwortung der Verfasserinnen und Verfasser sowie der Fachbereichsleitung. Arbeiten der Wissenschaftlichen Dienste geben nur den zum Zeitpunkt der Erstellung des Textes aktuellen Stand wieder und stellen eine individuelle Auftragsarbeit für einen Abgeordneten des Bundestages dar. Die Arbeiten können der Geheimschutzordnung des Bundestages unterliegende, geschützte oder andere nicht zur Veröffentlichung geeignete Informationen enthalten. Eine beabsichtigte Weitergabe oder Veröffentlichung ist vorab dem jeweiligen Fachbereich anzuzeigen und nur mit Angabe der Quelle zulässig. Der Fachbereich berät über die dabei zu berücksichtigenden Fragen.

Inhaltsverzeichnis

1.	Einleitung und Überblick	4
2.	Deutschland	4
2.1.	Aufbewahrung von Messengerkommunikation und Daten auf Diensthandys	4
2.2.	Nutzung elektronischer Kommunikation als Beweismittel in Kontrollgremien	6
2.2.1.	Vorlagepflicht der Bundesregierung	6
2.2.2.	Vorlagepflicht Dritter	8
2.2.3.	Technische Umsetzung der Nutzung elektronischer Kommunikation als Beweismittel	9
3.	Dänemark	10
3.1.	Aufbewahrung von Messengerkommunikation und Daten auf Diensthandys	10
3.2.	Nutzung elektronischer Kommunikation als Beweismittel in Kontrollgremien	11
4.	Schweden	12
4.1.	Aufbewahrung von Messengerkommunikation und Daten auf Diensthandys	12
4.2.	Nutzung elektronischer Kommunikation als Beweismittel in Kontrollgremien	14
4.2.1.	Aufgaben und Befugnisse der Kontrollgremien	14
4.2.2.	Technische Umsetzung der Nutzung elektronischer Kommunikation als Beweismittel	15
5.	Großbritannien	16
5.1.	Aufbewahrung von Messengerkommunikation und Daten auf Diensthandys	16
5.2.	Nutzung elektronischer Kommunikation als Beweismittel in Kontrollgremien	17

1. Einleitung und Überblick

Die Wissenschaftlichen Dienste des Deutschen Bundestags wurden gebeten darzustellen, wie und aufgrund welcher Regelungen die Kommunikation von **obersten Regierungsbehörden** und Regierungsvertretern über **Messengerdienste und SMS** in Deutschland und ausgewählten anderen Staaten aufbewahrt und veraktet wird. Ferner soll geklärt werden, welche Regelungen für die Aufbewahrung von **Daten auf den Diensthandys** von Regierungsmitgliedern, Staatssekretärinnen und Staatssekretären gelten. Außerdem soll darauf eingegangen werden, wie diese Daten in rechtlicher und technischer Hinsicht von **Kontrollgremien**, z.B. einem Parlamentarischen Untersuchungsausschuss, als **Beweismittel** genutzt werden können und wie dabei **Persönlichkeitsrechten** und dem **Schutz personenbezogener Daten** Rechnung getragen wird.

Im Folgenden werden die aufgeworfenen Fragen zunächst mit Blick auf **Deutschland** (Punkt 2.) beantwortet. Sodann wird auf die jeweilige Lage in **Dänemark** (Punkt 3.), **Schweden** (Punkt 4.) und **Großbritannien** (Punkt 5.) eingegangen. Die Ausführungen zu den letzten drei Punkten beruhen auf Angaben der parlamentarischen Dienste in den jeweiligen Staaten.

2. Deutschland

2.1. Aufbewahrung von Messengerkommunikation und Daten auf Diensthandys

In Deutschland gibt es **keine spezifischen gesetzlichen Regelungen** über die Aufbewahrung und Veraktung der **elektronischen Kommunikation** von Regierungsmitgliedern, Ministerien oder Ministerialbeamten. Es gelten die aus dem Grundgesetz¹ abgeleiteten allgemeinen **Grundsätze einer ordnungsgemäßen Aktenführung**, die eine einheitliche und **vollständige Dokumentation** des Verwaltungshandelns einschließen.² Diese Grundsätze werden für die Bundesministerien durch eine **Gemeinsame Geschäftsordnung (GGO)**³ sowie die **Richtlinie für das Bearbeiten und Verwalten von Schriftgut in Bundesministerien (Registerrichtlinie (RegR))**⁴ näher konkretisiert. Bei diesen Vorschriften handelt es sich nicht um Gesetze oder Rechtsverordnungen, sondern um reines **Binnenrecht der Verwaltung**, mit der diese ihre eigenen Angelegenheiten regelt. Die

1 Grundgesetz für die Bundesrepublik Deutschland (Grundgesetz - GG) in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, zuletzt geändert durch Artikel 1 des Gesetzes vom 19. Dezember 2022 (BGBl. I S. 2478).

2 Zu den Rechtsgrundlagen dieser Pflicht und ihren Ausprägungen im Einzelnen vgl. Wissenschaftliche Dienste des Deutschen Bundestages, „Grundsätze der Aktenführung in der Bundesverwaltung“, Sachstand vom 29. September 2023, [WD 3 - 3000 - 108/23](#), S. 3 ff.

3 Gemeinsame Geschäftsordnung der Bundesministerien ([GGO](#)), in der Form der Bekanntmachung vom 30. August 2000, GMBL. S. 526 (Nr. 28), zuletzt geändert durch Art. 1 des Beschl. vom 15. Mai 2024 (GMBL 2024 Nr. 19, S. 386).

4 Richtlinie für das Bearbeiten und Verwalten von Schriftgut (Akten und Dokumenten) in Bundesministerien ([RegR](#)), Beschluss des Bundeskabinetts vom 11. Juli 2001.

Bundesregierung hat nach eigener Auskunft **keine gesonderten Regelungen** zur Nutzung von Messenger-Diensten in Bundesministerien getroffen, die über die RegR hinausgehen.⁵

Die **RegR** ergänzt die GGO und regelt das Bearbeiten von Geschäftsvorfällen und das Verwalten von Schriftgut in den Bundesministerien.⁶ Sie soll ein **sachgerechtes und wirtschaftliches Bearbeiten und Verwalten von Schriftgut** sicherstellen, wobei sie neben der **konventionellen (papierbezogenen)** Bearbeitung gleichzeitig die **IT-gestützte Vorgangsbearbeitung und Verwaltung von elektronischen Dokumenten und Akten** berücksichtigt.⁷ Zum **Schriftgut** gehören **alle bei der Erfüllung von Aufgaben des Bundes erstellten oder empfangenen Dokumente**, unabhängig von der Art des Informationsträgers und der Form der Aufzeichnung.⁸ Als **Dokument** gilt **jedes einzelne Schriftstück, egal ob papiergebunden oder elektronisch erstellt und verwaltet, ferner Fax, E-Mail, SMS, Messengernachrichten⁹, Datenbanken und andere Dateien**, einschließlich ergänzender Angaben (z. B. Metainformationen), die zum Verständnis der Informationen notwendig sind.¹⁰ Alle **aktenrelevanten** Unterlagen sind so zu verakten und aufzubewahren, dass **jederzeit auf sie zurückgegriffen** werden kann.¹¹ Im Fall von Messengerkommunikation kann dies – wie bei Telefonaten – mittels eines nachträglichen Gesprächsvermerks geschehen.¹² **Aktenrelevanz** besitzen alle Informationen, die **für die inhaltliche Bearbeitung eines Verwaltungsvorgangs von Bedeutung** sind, also **Teil eines Verwaltungsvorgangs werden sollen**.¹³ In Abgrenzung dazu sind **Dokumente ohne Informationswert zu vernichten**, solche mit **nur geringem Informationswert** sind als **Weglegesache**¹⁴ zu behandeln.¹⁵

5 Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Clara Bünger, Nicole Gohlke, Dr. André Hahn, weiterer Abgeordneter und der Gruppe Die Linke – Drucksache 20/12549, 10. September 2024, [BT-Drs. 20/12836](#), S. 4 (Antwort auf Frage 7).

6 Vgl. § 1 Abs. 1 RegR.

7 Vgl. § 1 Abs. 2 RegR.

8 Vgl. § 3 RegR, Definition „Schriftgut“.

9 Die Bundesregierung vertritt ausdrücklich die Ansicht, dass behördliche Chats aus Messenger-Diensten aktenrelevante Dokumente i.S.d. RegR darstellen können, vgl. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Clara Bünger, Nicole Gohlke, Dr. André Hahn, weiterer Abgeordneter und der Gruppe Die Linke – Drucksache 20/12549, 10. September 2024, [BT-Drs. 20/12836](#), S. 4 (Antwort auf Frage 5).

10 Vgl. § 3 RegR, Definition „Dokument“.

11 Vgl. § 10 Abs. 1 Satz 1 RegR.

12 Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Clara Bünger, Nicole Gohlke, Dr. André Hahn, weiterer Abgeordneter und der Gruppe Die Linke – Drucksache 20/12549, 10. September 2024, [BT-Drs. 20/12836](#), S. 5 (Antwort auf Frage 11).

13 Schoch, Informationsfreiheitsgesetz, 3. Auflage 2024, § 2 Rn. 45; BVerwG, Urteil vom 28. Oktober 2021 - [10 C 3.20](#), Rn. 18.

14 Zu den Folgen der Behandlung als Weglegesache vgl. RegR, Anlage 1, Abs. 3, „Wgl = Weglegen“.

15 Vgl. § 10 Abs. 1 Satz 2 RegR.

Zu **Direktnachrichten** des Bundesministeriums des Innern und für Heimat (BMI) auf einer Kurznachrichten-Plattform entschied das Bundesverwaltungsgericht (BVerwG), dass die in diesem konkreten Fall streitgegenständlichen Nachrichten wegen ihres **Bagatelldcharakters** keine Aktenrelevanz besaßen und deshalb nicht zu amtlichen Zwecken aufzubewahren waren.¹⁶

2.2. Nutzung elektronischer Kommunikation als Beweismittel in Kontrollgremien

Die Wissenschaftlichen Dienste wurden ferner gebeten darzulegen, unter welchen rechtlichen Voraussetzungen Kontrollgremien, insbesondere ein Untersuchungsausschuss, die elektronische Kommunikation von obersten Bundesbehörden und Regierungsvertretern als Beweismittel nutzen können und wie dabei Persönlichkeitsrechten und dem Schutz personenbezogener Daten Rechnung getragen wird.

Ein Untersuchungsausschuss erhebt die **durch den Untersuchungsauftrag gebotenen Beweise** gemäß § 17 Abs. 1 Untersuchungsausschussgesetz (PUAG)¹⁷ aufgrund von **Beweisbeschlüssen**. Beweise sind zu erheben, wenn sie von einem **Viertel der Mitglieder des Untersuchungsausschusses** beantragt sind, **es sei denn**, die **Beweiserhebung** ist **unzulässig** oder das **Beweismittel** ist auch nach Anwendung der im PUAG vorgesehenen Zwangsmittel **unerreichbar**. Zwar darf ein Beweisbeschluss nicht ohne jegliche tatsächliche Grundlage „völlig ins Blaue hinein“ gestellt werden, jedoch gelten im Untersuchungsausschuss verglichen mit dem Strafprozess weniger strenge Anforderungen an die Bestimmtheit, so dass die einzelne Beweiserhebung **nicht auf bestimmte Tatsachen bezogen** sein muss, sondern darauf abzielen kann, zunächst „Licht ins Dunkel“ eines Untersuchungskomplexes zu bringen.¹⁸ Zugleich muss ein Untersuchungsausschuss den Beweisbeschluss so konkret und eingrenzend formulieren, wie es ihm möglich ist, etwa durch Angabe einer Zeitspanne, in der die relevanten Unterlagen entstanden sind, und durch Darlegung des konkreten staatlichen Fehlverhaltens, das Gegenstand der Untersuchung ist.¹⁹ Insbesondere einer Privatperson kann nicht zugemutet werden, selbst abzuschätzen, welche in ihrem Gewahrsam befindlichen Beweismittel von Bedeutung für einen Untersuchungsausschuss sind.²⁰

2.2.1. Vorlagepflicht der Bundesregierung

Die Bundesregierung und andere Stellen des Bundes sind vorbehaltlich verfassungsrechtlicher Grenzen auf Ersuchen **verpflichtet**, einem Untersuchungsausschuss **sächliche Beweismittel**, insbesondere die Akten, die den Untersuchungsgegenstand betreffen, **vorzulegen**.²¹ Zu den

16 BVerwG, Urteil vom 28. Oktober 2021 - [10 C 3.20](#), Rn. 18.

17 Untersuchungsausschussgesetz (PUAG) vom 19. Juni 2001 (BGBl. I S. 1142), zuletzt geändert durch Artikel 12 Absatz 1 des Gesetzes vom 21. Dezember 2020 (BGBl. I S. 3229).

18 BVerfG, Beschluss vom 17. Juni 2009 – 2 BvE 3/07 (= BVerfGE 124, 78 (116)).

19 Risse/Oehm, Das Recht des Untersuchungsausschusses auf Dokumentenvorlage, NJW 2021, 1847 (Rn. 29).

20 Georgii, in: Waldhoff/Gärditz, PUAG, 1. Auflage 2015, § 29 Rn. 15.

21 Vgl. § 18 Abs. 1 PUAG.

sächlichen Beweismitteln gehören neben Urkunden und sonstigen verkörperten Gedankenerklärungen auch Augenscheinsobjekte sowie die bei der Exekutive vorhandenen **Akten**.²²

Die Bundesexekutive ist gemäß höchstrichterlicher Rechtsprechung nicht zur Vorlage verpflichtet, soweit eine Beweiserhebung den **Kernbereich exekutiver Eigenverantwortung** berührt, da dieser der Regierung einen grundsätzlich nicht ausforschbaren Initiativ-, Beratungs- und Handlungsbereich garantiert.²³ Die Kontrollkompetenz eines PUA erstreckt sich daher grundsätzlich **nur auf bereits abgeschlossene Vorgänge** und umfasst nicht die Befugnis, in laufende Verhandlungen und Entscheidungsvorbereitungen einzugreifen.²⁴ Nach Abschluss der jeweiligen Entscheidung sind Informationen aus dem Vorfeld von Regierungsentscheidungen zwar nicht mehr im selben Maße geschützt wie in der Phase, in der die Kenntniserhebung Dritter diesen einen unmittelbaren Einfluss auf die Entscheidung verschaffen würde, doch auch bei abgeschlossenen Vorgängen ist eine Berufung auf den Kernbereich exekutiver Eigenverantwortung nicht ausgeschlossen.²⁵ Eine weitere Grenze findet die Vorlagepflicht im **Staatswohl**, das durch das Bekanntwerden geheimhaltungsbedürftiger Informationen gefährdet werden kann. In einem solchen Fall besteht die Vorlagepflicht weiterhin, soweit umfassende Vorkehrungen gegen das Bekanntwerden von Dienstgeheimnissen getroffen wurden.²⁶ Dies kann durch **Ausschluss der Öffentlichkeit**²⁷ und durch **Einstufung** der Beweismittel mit einem **Geheimhaltungsgrad**²⁸ geschehen. Einschränkungen der Vorlagepflicht können sich auch zum **Schutz der Grundrechte** ergeben. Dabei ist das betroffene Grundrecht gegen das Beweiserhebungsrecht des Untersuchungsausschusses abzuwägen, wobei zu berücksichtigen ist, dass ein hinreichender Grundrechtsschutz gegebenenfalls über den Ausschluss der Öffentlichkeit oder die Einstufung des Beweismittels erreicht werden kann.²⁹

Die **Entscheidung** über das Ersuchen auf Vorlage bestimmter sächlicher Beweismittel trifft der zuständige **Bundesminister** oder die zuständige **Bundesministerin**, soweit sie nicht durch Gesetz der **Bundesregierung** vorbehalten ist.³⁰ Wird das Ersuchen abgelehnt oder werden sächliche Beweismittel als Verschlussache eingestuft, ist der Untersuchungsausschuss über die **Gründe der Ablehnung** oder der Einstufung **schriftlich** zu unterrichten.³¹ Die Vorlage ist mit einer **Erklärung**

22 Gärditz, in: Waldhoff/Gärditz, PUAG, 1. Auflage 2015, § 18 Rn. 15.

23 BVerfG, Beschluss vom 16. Dezember 2020 - 2 BvE 4/18 (= BVerfGE 156, 270 (298 f.)).

24 BVerfG, a.a.O.

25 BVerfG, Beschluss vom 30. März 2004 - 2 BvK 1/01 (= BVerfGE 110, 199 (215 f.)).

26 BVerfG, Beschluss vom 16. Dezember 2020 - 2 BvE 4/18 (= BVerfGE 156, 270 (299 f.)).

27 Vgl. § 14 PUAG.

28 Vgl. § 15 PUAG.

29 BVerfG, Beschluss vom 17. Juni 2009 - 2 BvE 3/07 (= BVerfGE 124, 78 (125 f.)).

30 Vgl. § 18 Abs. 2 Satz 1 PUAG.

31 Vgl. § 18 Abs. 2 Satz 2 PUAG.

über die Vollständigkeit zu verbinden.³² Auf Antrag des Untersuchungsausschusses oder eines Viertels seiner Mitglieder entscheidet das **Bundesverfassungsgericht** über die **Rechtmäßigkeit der Ablehnung** eines Vorlageersuchens und der **Ermittlungsrichter** oder die **Ermittlungsrichterin des Bundesgerichtshofes** über die **Rechtmäßigkeit der Einstufung** einer Verschlussache.³³ **Gerichte und Verwaltungsbehörden** sind zur **Rechts- und Amtshilfe**, insbesondere zur Vorlage sächlicher Beweismittel, verpflichtet.³⁴ Über **Streitigkeiten** entscheidet auf Antrag des Untersuchungsausschusses oder eines Viertels seiner Mitglieder der **Ermittlungsrichter** oder die **Ermittlungsrichterin des Bundesgerichtshofes**.³⁵

2.2.2. Vorlagepflicht Dritter

Befindet sich ein Gegenstand, der als Beweismittel für die Untersuchung von Bedeutung sein kann, im **Gewahrsam eines Dritten** (etwa eines Telekommunikationsunternehmens oder eines Anbieters von OTT-Messaging-Diensten³⁶), so ist dieser **verpflichtet**, den Gegenstand auf Verlangen des Untersuchungsausschusses **vorzulegen und auszuliefern**.³⁷ Diese Pflicht besteht nicht, soweit das Beweismittel Informationen enthält, deren Weitergabe wegen ihres streng persönlichen Charakters für die Betroffenen unzumutbar ist.³⁸ Das Herausgabeverlangen kann sich erstrecken auf **bewegliche Sachen jeder Art**, auch **Datenträger** und **Computerausdrucke** sowie **Ton- und Bildträger**, ebenso auf nichtkörperliche Gegenstände wie **digital gespeicherte Informationen**, insbesondere **E-Mails auf dem Mailserver** des Providers.³⁹ Werden Gegenstände **nicht freiwillig** vorgelegt, so entscheidet auf Antrag des Untersuchungsausschusses oder eines Viertels seiner Mitglieder der Ermittlungsrichter oder die Ermittlungsrichterin des Bundesgerichtshofes über die **Beschlagnahme** und die **Herausgabe** an den Untersuchungsausschuss.⁴⁰

Wendet die Person, die den Gewahrsam innehat, ein, verlangte Beweismittel seien für die Untersuchung **nicht bedeutsam** oder **beträfen ein Geheimnis**, das nach § 14 Abs. 1 Nr. 1 bis 4 PUAG zum **Ausschluss der Öffentlichkeit** führen würde, so dürfen Ordnungs- und Zwangsmittel und die Herausgabe nur dann angeordnet werden, wenn das Beweismittel keine Informationen enthält, deren Weitergabe wegen ihres **streng vertraulichen Charakters** für die Betroffenen

32 Vgl. § 18 Abs. 2 Satz 3 PUAG.

33 Vgl. § 18 Abs. 3 PUAG.

34 Vgl. § 18 Abs. 4 Satz 1 PUAG.

35 Vgl. § 18 Abs. 4 Satz 2 PUAG.

36 Kommunikationsdienste, die unabhängig vom Zugangsprovider (Telekommunikationsunternehmen) über das Internet betrieben werden, werden auch als Over-the-Top-Dienste (OTT-Dienste) bezeichnet; dies sind insbesondere Messenger-Dienste.

37 Vgl. § 29 Abs. 1 Satz 1 PUAG.

38 Vgl. § 29 Abs. 1 Satz 2 PUAG.

39 Georgii, in: Waldhoff/Gärditz, PUAG, 1. Auflage 2015, § 29 Rn. 6.

40 Vgl. § 29 Abs. 3 Satz 1 PUAG.

unzumutbar ist, und der Untersuchungsausschuss für dieses Beweismittel den **Geheimhaltungsgrad GEHEIM** beschlossen hat.⁴¹

Die **Durchsicht** und die **Prüfung** der **Beweiserheblichkeit** der vorgelegten Beweismittel steht dem Untersuchungsausschuss zu.⁴² Beweismittel, die sich nach einmütiger Auffassung des Untersuchungsausschusses für die Untersuchung als **unerheblich** erweisen, sind der Person, die den Gewahrsam hatte, **unverzüglich zurückzugeben**.⁴³ Nach Durchsicht und Prüfung der Beweismittel kann der Untersuchungsausschuss die **Aufhebung der Einstufung** in den Geheimhaltungsgrad GEHEIM beschließen, soweit die Beweismittel für die Untersuchung **erheblich** sind. Betreffen sie ein Geheimnis, das zum Ausschluss der Öffentlichkeit führen würde, so darf der Untersuchungsausschuss die Aufhebung nur dann beschließen, wenn die **öffentliche Verwendung** der Beweismittel zur Erfüllung des Untersuchungsauftrages **unerlässlich** und **nicht unverhältnismäßig** ist.⁴⁴ Vor der Beschlussfassung ist die **Person**, die über das Beweismittel **verfügungsberechtigt** ist, zu **hören**.⁴⁵ **Widerspricht** sie der Aufhebung des Geheimhaltungsgrades GEHEIM, so hat die **Aufhebung** zu **unterbleiben**, wenn nicht der Ermittlungsrichter oder die Ermittlungsrichterin des Bundesgerichtshofes auf Antrag des Untersuchungsausschusses oder eines Viertels seiner Mitglieder sie für zulässig erklärt.⁴⁶

2.2.3. Technische Umsetzung der Nutzung elektronischer Kommunikation als Beweismittel

In welcher Weise die Nutzung elektronischer Kommunikation als Beweismittel im Rahmen eines Untersuchungsausschusses **technisch umgesetzt** wird, hängt davon ab, in welcher Form die beherrschten Informationen vorliegen.

Informationen, die sich im Gewahrsam der Bundesexekutive befinden, sind grundsätzlich **als Originalakte** und nur ausnahmsweise (etwa aufgrund mangelnder Transporteignung) als Kopie vorzulegen.⁴⁷ Soweit gelöschte Informationen, auf die sich der Untersuchungsauftrag erstreckt, noch lokal, d.h. in der verwaltungseigenen IT, gespeichert als **Löschkopie** oder **Logfile** (Protokoll-datei) vorhanden sind, kann auch auf diese zugegriffen werden.⁴⁸ Gleiches gilt, wenn diese Informationen noch auf **Servern** von Zugangs- oder Kommunikationsdiensteanbietern liegen.⁴⁹ Soweit Informationen erst sicht- bzw. lesbar gemacht werden müssen (etwa durch Entschlüsselung oder

41 Vgl. § 30 Abs. 1 PUAG.

42 Vgl. § 30 Abs. 2 Satz 1 PUAG.

43 Vgl. § 30 Abs. 1 Satz 2 PUAG.

44 Vgl. § 30 Abs. 3 PUAG.

45 Vgl. § 30 Abs. 4 Satz 1 PUAG.

46 Vgl. § 30 Abs. 4 Satz 2 PUAG.

47 Gärditz, in: Waldhoff/Gärditz, PUAG, 1. Auflage 2015, § 18 Rn. 17.

48 BGH Ermittlungsrichter 1 BGs 42/21 (1 ARs 1/20) - [Beschluss vom 29. Januar 2021](#).

49 So für das Strafverfahren BVerfG, Beschluss vom 16.06.2009 - 2 BvR 902/06 – (= BVerfGE 124, 43 (58 ff.)).

Überführung in ein gängiges Dateiformat), kann damit ein IT-Forensiker im Rahmen eines Sachverständigengutachtens⁵⁰ beauftragt werden.

3. Dänemark

3.1. Aufbewahrung von Messengerkommunikation und Daten auf Diensthandys

In Dänemark gibt es sowohl gesetzliche als auch untergesetzliche Vorschriften über die Aufbewahrung behördlicher Informationen und Unterlagen.

Das dänische **Gesetz über den Zugang zu Akten der öffentlichen Verwaltung (Offentlighedsloven)**⁵¹ gilt umfassend für sämtliche Aktivitäten der öffentlichen Verwaltung in Dänemark. Danach müssen Dokumente, die von einer Verwaltungsbehörde im Rahmen der administrativen Fallbearbeitung empfangen oder versandt werden, aufgezeichnet werden, sofern sie **für die Bearbeitung des Falls relevant** sind. Als Dokument gelten sowohl **verkörperte schriftliche Dokumente** als auch Materialien, die schriftliche Dokumente und Aufzeichnungen im Rahmen der administrativen Fallbearbeitung ersetzen. Die Definition eines Dokuments ist **technologieneutral**, so dass **auch SMS-Nachrichten** und ähnliche Kommunikation (wie z.B. **E-Mail oder Messenger-Chats**) eingeschlossen sind. Ob eine SMS-Nachricht oder ähnliche Kommunikation aufgezeichnet werden muss, hängt von einer spezifischen Bewertung des **Inhalts der Nachricht**, der **Natur des Falls**, auf den sich die Nachricht bezieht, und des Inhalts der **anderen in dem Fall aufgezeichneten Materialien** ab. Zudem spielt eine Rolle, ob die betreffenden Informationen **bereits** in anderen Falldokumenten **enthalten** sind. Ist ein Kommunikationsinhalt danach zwingend aufzuzeichnen, **kommt es nicht darauf an**, ob dieser Inhalt von einem **dienstlichen oder einem privaten Endgerät** gesendet oder empfangen wurde. **Entscheidend** für die Aufzeichnungspflicht ist die **Relevanz** einer Information für die **Fallbearbeitung**, nicht das Medium oder die Plattform, mittels derer die Kommunikation stattfand. Das Gesetz über den Zugang zu Akten der öffentlichen Verwaltung schreibt nicht die Verwendung eines bestimmten Dokumentenmanagementsystems vor, sondern verlangt stattdessen, dass das verwendete System Informationen zum Empfangs- oder Versanddatum des Dokuments und eine kurze thematische Beschreibung seines Inhalts enthalten muss.

Zusätzlich zu den soeben skizzierten gesetzlichen Aufzeichnungsregeln gibt es in Dänemark **Richtlinien für staatliche Behörden zur Aufbewahrung gelöschter E-Mails⁵² und SMS-Nachrichten⁵³**. Diese Richtlinien stellen sicher, dass **E-Mails, SMS-Nachrichten** und ähnliche Kommunikationsinhalte für einen bestimmten Zeitraum **aufbewahrt** werden, **unabhängig** davon, ob sie der **Aufzeichnungspflicht** unterliegen oder nicht. Die im September 2021 herausgegebenen E-Mail-Richtlinien **empfehlen** staatlichen Behörden, **lokal gelöschte E-Mails** von aktuellen Mitarbeitern,

50 Vgl. § 28 PUAG.

51 In dänischer Sprache [hier](#) abrufbar.

52 Justitsministeriet, Retningslinjer for statslige myndigheders opbevaring af slettede e-mails mv., September 2021, in dänischer Sprache [hier](#) abrufbar.

53 Justitsministeriet, Retningslinjer for statslige myndigheders opbevaring af SMS-beskeder mv., Mai 2024, in dänischer Sprache [hier](#) abrufbar.

Managern (Abteilungsleitern und höher), Ministern, ständigen Sekretären und Sonderberatern sowie die E-Mail-Konten ausgeschiedener Mitarbeiter – einschließlich ehemaliger Manager – **vor der endgültigen Löschung** für einen bestimmten Zeitraum **aufzubewahren**. Ziel dieser Richtlinien ist es, eine **einheitliche Praxis** zur Aufbewahrung gelöschter E-Mails und E-Mail-Konten ausgeschiedener Mitarbeiter zu gewährleisten, damit Behörden dem Verlangen einer Untersuchungskommission oder eines Untersuchungsausschusses, **auf nicht aufgezeichnete E-Mails zuzugreifen**, nachkommen können. Die **SMS-Richtlinien** betreffen die **Aufbewahrung von SMS-Nachrichten** und **ähnlichen Kommunikationsformen** (insbesondere Chats bei Messengerdiensten). Darin wird staatlichen Behörden **empfohlen**, Mitarbeiter anzuweisen, arbeitsbezogene **SMS-Nachrichten** für Zeiträume von **5 Jahren (Mitarbeiter)**, **10 Jahren (Manager der Besoldungsgruppe 37 oder höher)** oder **25 Jahren (Minister, Sonderberater und ständige Sekretäre)** nicht zu löschen. Wenn ein Mitarbeiter seine **Position verlässt** oder das **Telefon wechselt**, müssen seine **SMS- und Chat-Nachrichten**, die er mit **bestimmten Mitarbeitergruppen** (Minister, Sonderberater, ständige Sekretäre und andere leitende Beamte) ausgetauscht hat, **aufbewahrt** werden. Es wird davon ausgegangen, dass Mitarbeiter ihre **Diensttelefone** ausschließlich für **dienstbezogene Kommunikation** verwenden, einschließlich des Sendens und Empfangens von SMS- und Chat-Nachrichten. Wenn ein Mitarbeiter in **Ausnahmefällen** dienstbezogene Nachrichten auf seinem **persönlichen Telefon** gesendet oder empfangen hat, sollten auch diese Nachrichten gemäß den Richtlinien **aufbewahrt** werden. Die **SMS-Richtlinien** wurden **im Juli 2022** nach einer Untersuchungskommission herausgegeben, in der die Kommission nicht aufgezeichnete SMS-Nachrichten von den beteiligten Ministern und Beamten anforderte. Die Richtlinien sollen eine **einheitliche Praxis** zur **Aufbewahrung nicht aufgezeichneter SMS- und Chat-Nachrichten** durch staatliche Behörden sicherstellen, damit sie dem Verlangen einer Untersuchungskommission oder eines Untersuchungsausschusses, auf diese Informationen zuzugreifen, nachkommen können. Die E-Mail- und SMS-Richtlinien sind **rechtlich nicht bindend** und richten sich an staatliche Behörden. Die SMS-Richtlinien werden **jedoch durch ministerielle Anweisungen für Minister und Mitarbeiter verbindlich**.

3.2. Nutzung elektronischer Kommunikation als Beweismittel in Kontrollgremien

Die Frage der Offenlegung von Dokumenten ergibt sich insbesondere im Zusammenhang mit externen Untersuchungen. Bei Untersuchungskommissionen und Untersuchungsausschüssen ist zu beachten, dass solche Kommissionen typischerweise gemäß dem **Gesetz über Untersuchungskommissionen und Untersuchungsausschüsse** eingerichtet werden. Danach gibt es eine **allgemeine Pflicht**, Materialien auf Anfrage einer Untersuchungskommission oder eines Untersuchungsausschusses **vorzulegen**. Der Begriff „Materialien“ wird dabei **weit ausgelegt** und umfasst neben **E-Mails** auch **SMS-Nachrichten** und **Messenger-Kommunikation**.

Die Verarbeitung personenbezogener Daten durch Untersuchungskommissionen und Untersuchungsausschüsse, die gemäß dem Gesetz über Untersuchungskommissionen und Untersuchungsausschüsse eingerichtet wurden, unterliegt der **Datenschutz-Grundverordnung (DSGVO)** und dem **dänischen Datenschutzgesetz**. Andere Arten externer Untersuchungen, wie rechtliche Untersuchungen, können ohne gesetzliche Grundlage eingerichtet werden. Allerdings kann der Ermittler in diesen Fällen nicht verlangen, dass öffentliche Behörden solche Dokumente vorlegen, die nicht bereits nach dem Gesetz über den Zugang zu Akten der öffentlichen Verwaltung zugänglich sind. Behörden stellen üblicherweise jedoch freiwillig Materialien für eine rechtliche Untersuchung bereit.

4. Schweden

Bevor auf die Einzelheiten zur Aufbewahrung behördlicher elektronischer Kommunikation in Schweden eingegangen wird, soll kurz erläutert werden, welche Aufgaben und Rollen das schwedische Verfassungsrecht jeweils Regierung, öffentlicher Verwaltung und Parlament zuweist.

Alle schwedischen **Regierungsbehörden** erhalten ihre **Aufträge von der Regierung** und sind dieser gegenüber **rechenschaftspflichtig**. Im Gegensatz zu den meisten anderen Ländern ist es schwedischen **Ministern** jedoch **nicht gestattet**, in die **Rechtsanwendung** bzw. die **Ausübung der behördlichen Befugnisse** einzugreifen. Die Regierung steuert die Behörden, indem sie **Leitlinien** für ihre Arbeit herausgibt, insbesondere in Form von **Verordnungen mit Anweisungen und jährlichen Haushaltsrichtlinien**, die ihre Zuständigkeiten, Betriebsziele und die ihnen zur Verfügung stehenden Mittel definieren. Jede Behörde handelt dann eigenverantwortlich innerhalb dieses Rahmens. Die Regierung **überwacht** die Tätigkeit der **öffentlichen Verwaltung** durch verschiedene Mechanismen und Behörden. Über die **reguläre Aufsicht** hinaus wird die **außergewöhnliche Aufsicht** im Auftrag der Regierung vom **Justizkanzler** ausgeübt.

Eine der **Hauptaufgaben** des **schwedischen Parlaments**, des Riksdag, besteht darin, die **parlamentarische Kontrolle** über die Arbeit der **Regierung** und der **öffentlichen Verwaltung** auszuüben. Die Regierung ist dem Parlament gegenüber rechenschaftspflichtig. Gleichwohl sieht das schwedische Verfassungssystem **keine parlamentarischen Untersuchungsausschüsse** im strengen Wortsinn vor. Die verschiedenen **Instrumente** der parlamentarischen Kontrolle sind in der schwedischen Verfassung⁵⁴ festgelegt und umfassen **Prüfungen**, z.B. durch den Verfassungsausschuss, die Parlamentarischen Ombudsmänner und den Nationalen Rechnungshof.

4.1. Aufbewahrung von Messengerkommunikation und Daten auf Diensthandy

In Schweden gibt es **keine spezifischen gesetzlichen Bestimmungen** zur **Aufbewahrung und Archivierung elektronischer Kommunikation** von Regierungsmitgliedern, Ministerien oder Ministerialbeamten. Die allgemeinen Grundsätze zu amtlichen Dokumenten und zum Archivmanagement, die sich aus dem **Pressegesetz**⁵⁵ und dem **Archivgesetz**⁵⁶ ergeben, gelten für die **Regierung** und die **Regierungsbehörden** sowie für **alle anderen staatlichen Behörden**.

Nach den Bestimmungen des Pressegesetzes hat jedermann das Recht auf Zugang zu **amtlichen Dokumenten**. Ein Dokument ist amtlich, wenn es sich im **Gewahrsam einer Behörde** befindet und nach bestimmten Regeln als von einer solchen Behörde **empfangen oder erstellt** gilt. Die Regelung im Pressegesetz ist **technologieneutral** und gilt daher für Dokumente **unabhängig vom Medium**, z.B. E-Mails, Sprachnachrichten, Textnachrichten und Blogbeiträge.

54 Die schwedische Verfassung besteht aus insgesamt vier Grundgesetzen (Grundlagar), nämlich dem Grundgesetz zur Regierungsform ([Regeringsformen](#), erlassen 1975), dem Thronfolgesetz ([Successionsordningen](#), erlassen 1810, revidiert 1979), dem Pressegesetz ([Tryckfrihetsförordningen](#), erlassen 1949) und dem Grundgesetz über die Freiheit der Meinungsäußerung ([Yttrandefrihetsgrundlagen](#), erlassen 1991).

55 Das Pressegesetz ist Teil des schwedischen Verfassungsrechts, siehe vorherige Fn.

56 Arkivlag (1990:782), schwedische Fassung abrufbar [hier](#).

Kommunikation, die **namentlich** an eine **Person in einer öffentlichen Behörde** gerichtet ist, gilt als amtliches Dokument, wenn sie eine Angelegenheit oder ein Problem betrifft, das von der Behörde behandelt werden soll. Es spielt dabei **keine Rolle**, ob ein **privates oder dienstliches Mobiltelefon** verwendet wird; **entscheidend** ist der **Inhalt des Dokuments**. Wenn eine Textnachricht **dienstliche Angelegenheiten** betrifft und **von einem Regierungsmitglied oder Beamten erstellt oder empfangen** wird, gilt die Nachricht als **von der Behörde erstellt oder empfangen**. Ist die Kommunikation dagegen **ausschließlich** für den Empfänger in einer **anderen Eigenschaft** als der eines Beamten bestimmt – wie z.B. ein Minister in seiner Funktion als Mitglied einer politischen Partei – gilt sie **nicht als amtliches Dokument**. Diese Bestimmung wird oft als „**politische Ausnahme**“ bezeichnet. Sie soll sicherstellen, dass Kommunikationsvorgänge, die **eindeutig parteipolitischen Aktivitäten** zuzuordnen sind, selbst dann **nicht für die Allgemeinheit zugänglich** sind, wenn an ihnen ein Beamter beteiligt ist und sie ein Thema betreffen, für das er in seiner Funktion als Beamter verantwortlich ist. Nur Kommunikationsinhalte über **spezifische Behördenangelegenheiten** sollen als amtliche Dokumente behandelt werden. Verwendet ein Minister in sozialen Medien ein privates Profil, so ist er **persönlich** dafür **verantwortlich**, dass diejenigen Inhalte, die die Anforderungen an ein amtliches Dokument erfüllen, gemäß den geltenden Vorschriften registriert, aufbewahrt und archiviert werden.

Amtliche Dokumente sind in der Regel zu **registrieren**, sobald sie von **einer öffentlichen Behörde empfangen** oder **erstellt** wurden, und sodann **aufzubewahren** und zu **archivieren**.

Die Archive öffentlicher Behörden, einschließlich der Regierung und der Regierungsstellen, sind so zu verwalten, dass das **Recht auf Zugang zu offiziellen Dokumenten** effektiv gewährleistet ist. Insbesondere dürfen **keine Maßnahmen** ergriffen werden, die zu einem **Verlust wesentlicher Daten** oder der **Möglichkeit zur Beurteilung der Authentizität** des Dokuments führen. So kann beispielsweise das Ausdrucken eines elektronischen Dokuments auf Papier und das anschließende Vernichten der elektronischen Version zum Verlust von Metadaten oder einer elektronischen Signatur führen, die in der gedruckten Version nicht sichtbar sind. **Aufnahmen**, also Informationen, die nur unter Verwendung technischer Hilfsmittel gelesen, gehört oder anderweitig wahrgenommen werden können, müssen **nicht in einer unmittelbar wahrnehmbaren Form** als physische Gegenstände in der Behörde aufbewahrt werden. Es reicht vielmehr aus, wenn die Aufnahme **zugänglich** ist, um durch die Verwendung technischer Hilfsmittel in eine lesbare, hörbare oder anderweitig wahrnehmbare Form umgewandelt zu werden.

Dass ein Dokument **amtlich** ist, bedeutet im Übrigen **nicht zwingend**, dass es auch **öffentlich zugänglich** ist. Informationen in amtlichen Dokumenten können gemäß den Bestimmungen des **Gesetzes über den öffentlichen Zugang zu Informationen und Geheimhaltung**⁵⁷ als geheim eingestuft werden, wodurch das Recht auf Zugang zu diesen Dokumenten begrenzt wird. Die Geheimhaltungsvorschriften bezwecken sowohl den **Schutz öffentlicher Interessen** (z.B. nationale Sicherheit und öffentliches Finanzinteresse) als auch den **Schutz von Informationen** über die **persönlichen oder finanziellen Verhältnisse** einer **natürlichen Person**.

57 Offentlighets- och sekretesslag (2009:400, eine schwedische Fassung kann [hier](#) abgerufen werden, eine englischsprachige Erläuterung des Gesetzes [hier](#)).

4.2. Nutzung elektronischer Kommunikation als Beweismittel in Kontrollgremien

Den gesetzlichen Bestimmungen zufolge steht die Einstufung eines Dokuments als geheim seiner **Offenlegung** gegenüber dem **Parlament (Riksdag)** oder der **Regierung** nicht entgegen. Diese Ausnahme gilt umfassend und ohne Einschränkungen für jegliche Informationen, die Riksdag oder Regierung für ihre Arbeit benötigen. Zudem legt das Gesetz fest, dass eine Behörde als geheim eingestufte Informationen jedenfalls dann einer anderen Behörde gegenüber offenlegen kann, wenn eine gesetzliche oder verordnungsrechtliche Verpflichtung zur Bereitstellung solcher Informationen besteht.

4.2.1. Aufgaben und Befugnisse der Kontrollgremien

Die schwedische Verfassung kennt eine Reihe unterschiedlicher Kontrollgremien, die sich in ihren Aufgabenstellungen und infolgedessen auch in den Möglichkeiten der Informationsbeschaffung unterscheiden.

So soll der **Verfassungsausschuss** die **Leistung der Minister** bei der Ausführung ihrer amtlichen Aufgaben (einschließlich der Entscheidungen und Maßnahmen, die sie in ihrer Funktion als Premierminister, Minister oder Leiter eines Ministeriums getroffen haben) und die **Behandlung von Regierungsangelegenheiten** (einschließlich der Maßnahmen, die von Beamten innerhalb der Regierung getroffen wurden) prüfen. Ausdrücklich **nicht zuständig** ist der Verfassungsausschuss für Maßnahmen und Entscheidungen, die Minister nicht in Ausübung ihres Amtes, sondern in ihrer **Eigenschaft als Privatpersonen oder Parteipolitiker** treffen. Für seine Prüfung kann der Ausschuss auf **Protokolle** der Entscheidungen in Regierungsangelegenheiten und die **dazugehörigen Dokumente** sowie auf **andere Regierungsdokumente**, die der Ausschuss für seine Prüfung als **notwendig erachtet**, zugreifen. Dieses Recht umfasst sowohl **offizielle** als auch **nicht-offizielle Dokumente** (z. B. Memoranden und Entscheidungsentwürfe). Nicht-offizielle Dokumente gelten als offiziell, sobald sie dem Ausschuss vorgelegt werden. Die **Einstufung als geheim** stellt, wie oben erläutert, **kein Hindernis** für die Vorlage von Dokumenten vor dem Verfassungsausschuss dar. Dem Zuständigkeitszuschnitt des Ausschusses entsprechend unterliegen Dokumente im Gewahrsam der Regierung dann nicht seinem Zugriff, wenn sie unter die sogenannte **politische Ausnahme** (siehe oben 3.1.) fallen oder **rein privater Natur** sind. Dem **Schutz personenbezogener Daten** und dem Schutz staatlicher Interessen trägt der Umstand Rechnung, dass die Sitzungen der Ausschüsse im Riksdag in der Regel unter **Ausschluss der Öffentlichkeit** stattfinden, also weder die Öffentlichkeit noch die Medien an ihnen teilnehmen dürfen.

Alle schwedischen Regierungsbehörden werden von den **parlamentarischen Ombudsleuten** überwacht und vom **Nationalen Rechnungsprüfungsamt (NAO)** geprüft. Beide Behörden sind dem **Riksdag unterstellt** und haben weitreichende **Rechte auf Zugang zu Dokumenten und Informationen**. Die parlamentarischen Ombudsleute überwachen die **ordnungsgemäße Anwendung von Gesetzen und anderen Bestimmungen** durch öffentliche Stellen. Die rechtliche Grundlage dafür findet sich im Verfassungsrecht⁵⁸ und dem einfachen Recht.⁵⁹ Gemäß der Verfassung hat

58 Grundgesetz zur Regierungsform ([Regeringsformen](#), erlassen 1975).

59 Gesetz (2023:499) mit Anweisungen für die parlamentarischen Ombudsleute, schwedische Fassung abrufbar [hier](#).

ein Ombudsmann das Recht, auf die **Aufzeichnungen** und andere **Dokumente von Gerichten und Verwaltungsbehörden** zuzugreifen, und umgekehrt jede Behörde oder Person unter der Aufsicht des Ombudsmanns die Pflicht, ihm die gewünschten Informationen und Einschätzungen zur Verfügung stellen. Die Aufsicht der Ombudsleute erstreckt sich **nicht** auf die **Regierung** oder die **Minister**.

Das **NAO** prüft die Tätigkeit der gesamten Exekutive. Die rechtlichen Grundlagen für die Prüfung finden sich erneut in der Verfassung⁶⁰ und im einfachen Recht⁶¹. Gemäß der Verfassung müssen **zentrale Regierungsbehörden** dem Nationalen Rechnungsprüfungsamt die für seine Prüfung erforderlichen Informationen zur Verfügung stellen. Die Verpflichtung öffentlicher Behörden, Dokumente den parlamentarischen Ombudsleuten und dem Nationalen Rechnungsprüfungsamt bereitzustellen, gilt **unabhängig davon**, ob die Dokumente offiziell sind oder nicht. Geheimhaltungsvorschriften stehen der Herausgabe von Informationen an eine Aufsichts- oder Prüfungsbehörde nicht entgegen, wenn die Behörde die Information für die Ausübung der Aufsicht oder die Durchführung einer Prüfung benötigt.

Gibt eine Behörde als geheim eingestufte Informationen an eine **Aufsichts- und Prüfungsbehörde** weiter, so hat die empfangende Behörde dieselben Geheimhaltungsbestimmungen anzuwenden wie die übergebende Behörde (sogenannte **Sekundärgeheimhaltung**). Beantragt eine Person Zugang zu den von der Aufsichts- oder Prüfungsbehörde erhaltenen Informationen, prüft und entscheidet die Behörde unabhängig, ob die Informationen gemäß der anzuwendenden Geheimhaltungsbestimmungen geheim sind. Von der Sekundärgeheimhaltung **ausgenommen** sind Informationen, die **Teil einer Entscheidung der empfangenden Behörde** geworden sind. Informationen, auf die **parlamentarische Ombudsleute** im Zuge ihrer Tätigkeit stoßen, unterliegen nur dann der Geheimhaltung, wenn anzunehmen ist, dass **öffentliche oder private Interessen** ansonsten **erheblich beeinträchtigt** werden oder **schweren Schaden** nehmen könnten.

4.2.2. Technische Umsetzung der Nutzung elektronischer Kommunikation als Beweismittel

Ein amtliches Dokument, das veröffentlicht werden soll, ist dem Antragsteller nach den Regelungen des Pressegesetzes **so zur Verfügung zu stellen**, dass das Dokument **gelesen, gehört oder anderweitig wahrgenommen** werden kann. Ist dies ohne technische Hilfsmittel nicht möglich, so muss die Behörde die erforderlichen Hilfsmittel bereitstellen. Dabei kann eine zur automatisierten Verarbeitung bestimmte **Aufnahme** in gedruckter Form bereitgestellt oder auf einem Bildschirm angezeigt werden.

Die **technischen Mittel**, mit denen **elektronische Kommunikation** im Rahmen der **parlamentarischen Kontrolle** als Beweismittel verwendet wird, sind **nicht spezifisch geregelt**. Vielmehr gelten die oben unter 4.1. dargelegten **allgemeinen Anforderungen** für die Aufbewahrung substantzieller Informationen sowie die soeben skizzierte behördliche Pflicht, ggf. die **Umwandlung** in eine **lesbare, hörbare oder anderweitig wahrnehmbare Form** zu ermöglichen. Um Sicherheitsinteressen

60 Grundgesetz zur Regierungsform ([Regeringsformen](#), erlassen 1975).

61 Gesetz (2002:1022) über die Prüfung staatlicher Aktivitäten, schwedische Fassung [hier](#) abrufbar.

Rechnung zu tragen, können bestimmte Dokumente zur Überprüfung beispielsweise in den Räumlichkeiten der Regierungsstellen zugänglich gemacht werden, anstatt sie herauszugeben.

Da ein Dokument nur gelöscht werden darf, wenn es nicht gemäß den geltenden Vorschriften (siehe oben 4.1.) aufbewahrt werden muss, wird ein **ordnungsgemäß gelöscht Dokument** als **nicht im öffentlichen Interesse liegend** betrachtet und somit **kein Zugriff** auf den Inhalt des entsorgten Dokuments gewährt. Selbst wenn es möglich wäre, die ordnungsgemäß entsorgten Informationen aus **Sicherungskopien wiederherzustellen**, besteht **keine Verpflichtung** für die Behörde, dies zu tun. **Sicherungskopien** gelten nach den Vorschriften des Pressegesetzes **nicht als öffentliche Dokumente**. Der Zweck von Sicherungskopien besteht darin, Informationen wiederherzustellen, die aufgrund technischer Ausfälle oder Sabotage, d.h. unbeabsichtigtem Verlust von Informationen, verloren gegangen sind. In Fällen von **unsachgemäß gelöschten Dokumenten/Informationen** hat das schwedische Oberste Verwaltungsgericht erklärt, dass die Behörde **grundsätzlich verpflichtet** ist, sie **so weit wie möglich aus vorhandenen Sicherungskopien wiederherzustellen**. Es gibt jedoch keine rechtliche Grundlage, die eine Behörde allgemein verpflichtet, gelöschte Dokumente wiederherzustellen.

5. Großbritannien

5.1. Aufbewahrung von Messengerkommunikation und Daten auf Diensthandy

Die Vorschriften für Minister und Beamte in Bezug auf nicht regierungseigene Kommunikationskanäle (NCCC)⁶² sind in einer im März 2023 veröffentlichten Richtlinie⁶³ festgelegt.

Inwieweit und unter Beachtung welcher Regeln Minister und Beamte über NCCCs kommunizieren dürfen, hängt danach vom Geheimhaltungsgrad der Kommunikation ab (zum Beispiel streng geheim). Die in der Richtlinie niedergelegten Regeln lassen sich wie folgt tabellarisch zusammenfassen:

Vertraulichkeitsgrad	Zugriff über dienstliches Endgerät	Zugriff über ein privates Endgerät
GEHEIM / STRENG GEHEIM	verboten	verboten
AMTLICH: bedeutende Information und/oder Information mit weiteren Kennzeichnungen (z.B. SENSIBEL)	Verwendung unter Anwendung besonderer Sorgfalt und angemessener Berücksichtigung der Archivierungspflichten	Nur in besonderen Ausnahmefällen zulässig. Jede Verwendung sollte der zuständigen Stelle für Wissens- und Informationsmanagement sowie

62 Non-corporate communication channels (NCCC) umfassen alle Kommunikationsmittel, die nicht von der Regierung bzw. der Verwaltung selbst betrieben werden, also z.B. Messenger-Apps, private E-Mails und SMS.

63 Cabinet Office, Using non-corporate communication channels (e.g. WhatsApp, private email, SMS) for government business, Richtlinie, 30. März 2023, in englischer Fassung abrufbar [hier](#).

		dem Dienstvorgesetzten angezeigt werden.
AMTLICH: Logistische oder nicht bedeutsame Information	Erlaubt	Erlaubt bei angemessener Berücksichtigung eigener Sicherheitspflichten

Bedeutende Informationen, die Regierungsstellen, Minister oder Beamte über NCCCs versenden oder erhalten, sollten gemäß der Richtlinie in eigenen Systemen der Regierung festgehalten und **aufbewahrt** werden. Die handelnden Personen sind **persönlich dafür verantwortlich**, basierend auf professionellem Urteilsvermögen und dem Kontext **zu entscheiden**, ob ein Kommunikationsinhalt zu **speichern** ist **oder nicht**. Bemerkt ein Minister oder Beamter im Verlauf einer elektronisch geführten Unterhaltung, dass die Gesprächsinhalte bedeutender werden, so sollte er die weitere Konversation entweder auf ein **durch die Regierung selbst betriebenes Kommunikationsmittel verlagern** oder sicherstellen, dass wichtige Inhalte anschließend **in einem eigenen System der Regierung gespeichert** werden. Das Festhalten bedeutender Informationen kann auf vielen verschiedenen Wegen erfolgen, also etwa **durch Kopieren, Weiterleiten oder das Anfertigen eines Screenshots (Bildschirmaufnahme)**. Alternativ kann der wesentliche Inhalt auch als **neue Nachricht, Notiz oder Dokument** in einem regierungseigenen Speichersystem angelegt werden. Minister oder hochrangige Beamte können diese Aufgaben auf die **Verwaltung ihres Hauses** übertragen. Stets ist darauf zu achten, dass der **Umfang der Speicherung** in einem **angemessenen Verhältnis** zum **Umfang der Nutzung von NCCC** steht. Insbesondere ist sicherzustellen, dass die Funktion „verschwindende Nachrichten“ die Einhaltung der Aufzeichnungs- oder Transparenzverpflichtungen nicht beeinträchtigt.

Diese Regeln gelten umfassend für alle Personen, die in der Zentralregierung arbeiten, einschließlich **aller Beamten, Staatssekretäre und des Premierministers**. Sie wurden 2023 nach der Veröffentlichung eines Berichts des Information Commissioner's Office (ICO)⁶⁴ eingeführt. Dem Bericht war eine einjährige Untersuchung der Verwendung von NCCCs durch Beamte und Minister im Gesundheitsministerium während der Covid-Pandemie vorausgegangen. Dabei stellte sich heraus, dass es während dieses Zeitraums keine klaren Kontrollmechanismen gab und dass es aufgrund der Verwendung von NCCCs für offizielle Kommunikation zu einem **erheblichen Verlust an Transparenz bei der Regierungsentscheidung** kam.

5.2. Nutzung elektronischer Kommunikation als Beweismittel in Kontrollgremien

Inhalte aus NCCC-Kommunikationen können als **schriftliche Beweismittel** in Untersuchungsausschüsse eingebracht werden. Dazu müssen die Nachrichten aus dem jeweiligen NCCC kopiert, verschriftlicht und an **formelle Vorgaben** des Ausschusses angepasst werden. Eine typische Beschreibung der formellen Vorgaben für Beweismittel, die ein Ausschuss akzeptiert, ist die

64 Information Commissioners Office, Behind the scenes: maintaining government transparency and data security in the age of messaging apps, Bericht, 11. Juli 2022, englische Fassung abrufbar [hier](#).

Präambel des Aufrufs zur Vorlage von Beweismitteln des Modernisierungsausschusses⁶⁵. Danach sollen Beweise z.B. nicht bereits an anderer Stelle veröffentlicht worden sein.

Zudem müssen alle Einreichungen bestimmte **technische Vorgaben** einhalten. Es dürfen nur einzelne Word-, ODT- oder RTF-Dateien mit einem Umfang von nicht mehr als 25 MB an einen Ausschuss übermittelt werden. Die Dateien dürfen keine Logos enthalten.

Jede **Weitergabe personenbezogener Daten** muss den Vorgaben des Datenschutzgesetzes 2018⁶⁶ und der britischen Datenschutzgrundverordnung (UK GDPR)⁶⁷ genügen.⁶⁸ Diese entsprechen den Anforderungen, die durch die EU-Datenschutzgrundverordnung (DS-GVO)⁶⁹ postuliert werden. Im Falle von Untersuchungsausschüssen ist die Weitergabe regelmäßig aufgrund von **Einwilligung** oder wegen eines **überwiegenden öffentlichen Interesses** zulässig.

Die britischen Gesetze sehen zusätzliche Schutzvorkehrungen für **besondere Kategorien personenbezogener Daten** vor, wozu Angaben über die **politischen Ansichten**, die **religiösen** oder **philosophischen Überzeugungen** und die **sexuelle Orientierung** einer Person gehören. Um besondere Kategorien personenbezogener Daten zu verarbeiten, muss eine rechtmäßige Grundlage gemäß Artikel 6 UK GDPR sowie eine der in Artikel 9 UK GDPR genannten separaten Bedingungen für die Verarbeitung vorliegen. Eine der Bedingungen ist die **ausdrückliche Einwilligung**. Es gibt neun weitere Bedingungen, darunter ein **erhebliches öffentliches Interesse**. Diese Fälle kommen bei der Weitergabe an Untersuchungsausschüsse zum Tragen.

65 Pre-Ambel of the Modernisation Committee's call for evidence, abrufbar [hier](#).

66 Data Protection Act 2018, englische Fassung abrufbar [hier](#).

67 UK General Data Protection Regulation, englische Fassung abrufbar [hier](#).

68 Vertiefende Informationen zur Funktionsweise des britischen Datenschutzrecht können einer im Oktober 2022 veröffentlichten Richtlinie des Information Commissioner's Office (ICO) entnommen werden, englische Fassung abrufbar [hier](#).

69 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung - DS-GVO), Verordnung Nr. 2016/679 des Europäischen Parlaments und Rates vom 27.4.2016, Amtsblatt L 119 vom 4.5.2016, S. 1, ber. Amtsblatt L 314 vom 22.11.2016, S. 72, Amtsblatt L 127 vom 23.5.2018, S. 2.