Bundesministerium
Landesverteidigung

bmlv.gv.at

Abteilung Präsidiale

[redacted]
Tel: 050201 - 0
Roßauer Lände 1, 1090 WIEN

[redacted]

Geschäftszahl: S90620/315-Präs/BürgSrv/2026 (2)
Datenschutz (D)DRINGEND

[redacted]

Betriebssysteme im ÖBH - Anfrage gemäß § 7 ff Informationsfreiheitsgesetz,
BESCHEID gem. § 11 Abs 1 IFG - Abweisung

B E S C H E I D

Über Ihren Antrag vom 1. März 2026 auf bescheidmäßige Erledigung nach § 11 Abs. 1 des Informationsfreiheitsgesetzes (IFG), BGBl. I Nr. 5/2024, bezogen auf Ihr Ersuchen auf Zugang zu Informationen gemäß §§ 7 ff IFG ergeht von der Bundesministerin für Landesverteidigung als zuständige Behörde folgender

SPRUCH:

Ihr Antrag auf Informationserteilung betreffend Verwendung der Betriebssysteme des Unternehmens Microsoft bzw. IBM OS/2 im Österreichischen Bundesheer (ÖBH) sowie die diesbezügliche Aufschlüsselung wird gemäß Art. 22a Abs. 2 des Bundes-Verfassungsgesetzes (B-VG) iVm § 6 Abs. 1 IFG wegen des Entgegenstehens von Geheimhaltungsgründen

abgewiesen.

BEGRÜNDUNG

Mit E-Mail vom 1. März 2026 ersuchten Sie gemäß § 7 Abs. 1 IFG Zugang zu folgenden Informationen:

„Sehr geehrte Damen und Herren,

hiermit beantrage ich gemäß § 7ff Informationsfreiheitsgesetz (IFG) die Erteilung folgender Information:

Wie viele Computersysteme beim Bundesheer verwenden eines der folgenden Betriebssysteme:

- *Microsoft Windows XP*
- *Microsoft Windows 98*
- *Microsoft Windows 95*
- *Microsoft Windows 3.1*
- *Microsoft MS-DOS*
- *IBM OS/2*

Ich bitte um Aufschlüsselung je Betriebssystem und die dazugehörige Anzahl der Computersysteme. Computersysteme die nicht eigenständig, aber Teil eines größeren Systems, Maschinerie oder Produktes sind, sollen auch mitgezählt werden."

Für den Fall der Nichterteilung der Informationen stellten Sie einen Eventualantrag auf bescheidmäßige Erledigung Ihres Antrags gemäß § 11 Abs. 1 IFG.

Mit Schreiben vom **20. März 2026**, GZ S90620/315-Präs/BürgSrv/2026 (1), wurde Ihnen zu Ihrem Antrag auf Informationserteilung Folgendes mitgeteilt:

„Sehr geehrter [redacted]

Zu Ihrer mit 1. März 2026 über die Plattform fragdenstaat.at eingebrachten Anfrage gemäß § 7 ff. Informationsfreiheitsgesetz (IFG) zu den Betriebssystemen innerhalb des Österreichischen Bundesheeres wird Ihnen von Seiten des Bundesministeriums für Landesverteidigung (BMLV) Folgendes mitgeteilt:

Jede verfügbare Information über die in den IKT-Systemen des ÖBH eingesetzte Hard- oder Software begünstigt feindliche Akteure im Cyberraum und schwächt damit die Fähigkeit zum militärischen Eigenschutz erheblich.

Informationen die technische Details (wie zB. Softwarebezeichnungen oder Versionen), Bestände oder Übersichtsdarstellungen über die IKT-Systeme des ÖBH beinhalten, unterliegen der Geheimhaltung gem. § 6 Abs. 1 Z 2 und Z 3 IFG."

Die Behörde hat erwogen:

I. Einschlägige Rechtsgrundlagen und Rechtsprechung:

Allgemeine rechtliche Erwägungen:

Art. 22a Abs. 2 des Bundes-Verfassungsgesetzes (B-VG) sieht vor, dass jedermann gegenüber den mit der Besorgung von Geschäften der Bundesverwaltung oder der Landesverwaltung betrauten Organen das Recht auf Zugang zu Informationen hat. Dies gilt nicht, soweit deren Geheimhaltung (siehe unten) geboten ist.

Information im Sinne des **§ 2 Abs. 1 IFG** ist jede amtlichen oder unternehmerischen Zwecken dienende Aufzeichnung im Wirkungsbereich eines Organs, im Tätigkeitsbereich einer Stiftung, eines Fonds oder einer Anstalt oder im Geschäftsbereich einer Unternehmung, unabhängig von der Form, in der sie vorhanden und verfügbar ist.

Gemäß **§ 3 Abs. 2 IFG** ist jenes informationspflichtige Organ, zu dessen Wirkungs- oder Geschäftsbereich die Information gehört, zuständig zur Gewährung des Zugangs zur Information.

Gemäß **§ 9 Abs. 1 IFG** ist die Information nach Möglichkeit in der begehrten, ansonsten in tunlicher Form möglichst direkt zugänglich zu machen; jedenfalls ist eine Information im Gegenstand zu erteilen. Die Verweisung auf bereits veröffentlichte oder auf anderem Weg einfacher zugängliche Informationen ist zulässig.

Gemäß **§ 11 Abs. 1 IFG** ist, wenn der Zugang zur Information nicht gewährt wird, auf schriftlichen Antrag des Informationswerbers vom informationspflichtigen Organ hierüber binnen zwei Monaten nach Einlangen des Antrags ein Bescheid zu erlassen. Als Verfahrensordnung, nach der der Bescheid zu erlassen ist, gilt das AVG, sofern das IFG keine Abweichungen vorsieht (vgl. ErlRV 2238 BlgNR 27. GP 12; zu § 11 IFG mit Verweis auf Art. I Abs. 1 iVm Abs. 2 Z 1 des Einführungsgesetzes zu den Verwaltungsverfahrensgesetzen 2008 – EGVG, BGBl. I Nr. 87).

Die Erläuterungen zum IFG (ErlRV 2238 BlgNR 27. GP 6) verweisen auf die Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte (EGMR) zu Art. 10 EMRK und legen fest, dass die Informationen bereits **„ready and available"**, dh bereits vorhanden und verfügbar sein müssen (vgl. zuletzt EGMR 30.1.2020, *Studio Monitori ua*, 44920/09, Rz 39 ff). Die Informationen müssen sich auf bereits bekannte Tatsachen beziehen und nicht erst erhoben, recherchiert, gesondert aufbereitet oder erläutert werden. Als noch nicht fertige Informationen können auch die im internen Entscheidungsprozess befindliche Vorentwürfe in einem Vorstadium und zum ausschließlichen Zweck der internen Entscheidungsfindung des entwurfserstellenden Organs anzusehen sein (AB 2420 BlgNR

27. GP 17). Der EGMR berücksichtigt im Rahmen seiner Entscheidungsfindung, ob die Verweigerung des Zugangs zu Informationen eine Verletzung von Art. 10 EMRK darstellt, stets den Umstand, ob die begehrte Information vorhanden und verfügbar ist und nicht etwa ein weiteres Sammeln von Daten notwendig ist (vgl. EGMR 8.11.2016, 18030/11, *Magyar Helsinki Bizottság/Ungarn*).

Der Zugang zur Information ist dann **nicht zu gewähren**, wenn gesetzliche **Geheimhaltungsgründe** bestehen.

Art. 22a Abs. 2 B-VG normiert auf Verfassungsebene die Grenzen der Informationsfreiheit. Gemäß **Art. 22a Abs. 2 B-VG** hat jedermann gegenüber den mit der Besorgung von Geschäften der Bundesverwaltung oder der Landesverwaltung betrauten Organen das Recht auf Zugang zu Informationen. Dies gilt jedoch nicht, soweit die Geheimhaltung von Informationen aus zwingenden staatlichen oder öffentlichen Gründen geboten ist; in concreto soweit deren Geheimhaltung aus zwingenden integrations- oder außenpolitischen Gründen, im Interesse der nationalen Sicherheit, der umfassenden Landesverteidigung oder der Aufrechterhaltung der öffentlichen Ordnung und Sicherheit, zur Vorbereitung einer Entscheidung, zur Abwehr eines erheblichen wirtschaftlichen oder finanziellen Schadens einer Gebietskörperschaft oder eines sonstigen Selbstverwaltungskörpers oder zur Wahrung überwiegender berechtigter Interessen eines anderen erforderlich und gesetzlich nicht anderes bestimmt ist. Die sonstigen Selbstverwaltungskörper (Art. 120a B-VG) sind in Bezug auf Angelegenheiten des eigenen Wirkungsbereiches nur gegenüber ihren Mitgliedern informationspflichtig.

Die angeführten Geheimhaltungstatbestände werden in **§ 6 Abs. 1 IFG** konkretisiert, wonach der beantragte Informationszugang nicht zu gewähren ist, **„soweit und solange"** dies aus einem in Z 1 bis 7 leg. cit. taxativ aufgezählten Geheimhaltungsgründe **„erforderlich und verhältnismäßig"** ist (vgl. *Koppensteiner/Lehne/Lehofer*, IFG § 6 Rz 82 ff) und **gesetzlich nicht anderes bestimmt ist**. Unter „erforderlich" ist geboten bzw. „notwendig" iS der grundrechtlichen Gesetzesvorbehalte der EMRK zu verstehen (AB 2420 BlgNR 27. GP 13). Die taxativ angeführten Geheimhaltungsgründe lauten wie folgt:

1. aus zwingenden integrations- oder außenpolitischen Gründen, insbesondere auch gemäß unmittelbar anwendbaren Bestimmungen des Rechts der Europäischen Union oder zur Einhaltung völkerrechtlicher Verpflichtungen,
2. im Interesse der nationalen Sicherheit,
3. im Interesse der umfassenden Landesverteidigung,
4. im Interesse der Aufrechterhaltung der öffentlichen Ordnung und Sicherheit,
5. im Interesse der unbeeinträchtigten Vorbereitung einer Entscheidung, im Sinne der unbeeinträchtigten rechtmäßigen Willensbildung und ihrer unmittelbaren Vorbereitung, insbesondere

a) von Handlungen des Bundespräsidenten, der Bundesregierung, der Bundesminister, der Staatssekretäre, der Landesregierung, einzelner Mitglieder derselben und des Landeshauptmannes, der Bezirksverwaltungsbehörden, der Organe der Gemeinde und der Organe der sonstigen Selbstverwaltungskörper,
b) im Interesse eines behördlichen oder gerichtlichen Verfahrens, einer Prüfung oder eines sonstigen Tätigwerdens des Organs sowie zum Schutz der gesetzlichen Vertraulichkeit von Verhandlungen, Beratungen und Abstimmungen,

6. zur Abwehr eines erheblichen wirtschaftlichen oder finanziellen Schadens der Organe, Gebietskörperschaften oder sonstigen Selbstverwaltungskörper oder
7. im überwiegenden berechtigten Interesse eines anderen, insbesondere
   a) zur Wahrung des Rechts auf Schutz der personenbezogenen Daten,
   b) zur Wahrung von Berufs-, Geschäfts- oder Betriebsgeheimnissen,
   c) zur Wahrung des Bankgeheimnisses (§ 38 des Bankwesengesetzes, BGBl. Nr. 532/1993),
   d) zur Wahrung des Redaktionsgeheimnisses (§ 31 des Mediengesetzes, BGBl. Nr. 314/1981) oder
   e) zur Wahrung der Rechte am geistigen Eigentum betroffener Personen.

Treffen die Voraussetzungen des § 6 Abs. 1 IFG nur auf einen Teil der Information zu, unterliegt nach § 6 Abs. 2 IFG nur dieser der Geheimhaltung. Besteht das Recht auf Information im Hinblick auf die beantragte Information nur zum Teil, ist die Information nach § 9 Abs. 2 insoweit zu erteilen, sofern dies möglich ist und damit kein unverhältnismäßiger Aufwand verbunden ist (AB 2420 BlgNR 27. GP 8).

Wie sich aus der Bestimmung des **Art. 22a Abs. 2 B-VG** ergibt, ist die Geheimhaltung bereits dann geboten, wenn auch nur ein einziges, in Art. 22a Abs. 2 B-VG genanntes, Interesse durch den Zugang zur Information beeinträchtigt werden würde (arg. „oder" in der Aufzählung der Ausnahmetatbestände, vgl. auch *Bußjäger* in *Bußjäger/Dworschak*, Informationsfreiheitsgesetz Art. 22a B-VG Rz 13: „(...) wenn *einer* der in Abs. 2 formulierten Gründe vorliegt").

Das gegenständliche Informationsbegehren ist somit dahingehend zu prüfen, ob

1. die begehrten Informationen vorhanden und verfügbar sind und gegebenenfalls,
2. ob einer Informationserteilung Geheimhaltungsverpflichtungen entgegenstehen.
3. Vornahme einer Interessenabwägung.

Rechtliche Erwägungen zur Interessenabwägung

Gem. **Art. 10 der Europäischen Menschenrechtskonvention (EMRK)** hat jedermann Anspruch auf freie Meinungsäußerung. In Zentrum des durch Art. 10 EMRK gewährleisteten Grundrechtssystems steht die individuelle Meinungsfreiheit: Jedermann hat das unveräußerliche Recht, sich durch den Austausch von Meinungen und

Informationen geistig und sozial zu verwirklichen. Auf der Seite des Äußernden manifestiert sich diese Freiheit als Meinungsäußerungsfreiheit; auf der Seite des Äußerungsempfängers als Informationsfreiheit. Der Schutzumfang dieses Grundrechts, das das Recht auf Freiheit der Meinung und das Recht auf Freiheit zum Empfang und zur Mitteilung von Nachrichten und Ideen ohne Eingriffe öffentlicher Behörden einschließt, umfasst sowohl reine Meinungskundgaben als auch Tatsachenäußerungen, aber auch Werbemaßnahmen.

Gemäß § 6 Abs. 1 IFG muss die Geheimhaltung erforderlich und verhältnismäßig sein. Es ist eine Interessenabwägung vorzunehmen, wobei diese im letzten Satz des Abs. 1 näher bestimmt wird: Es sind sämtliche in Betracht kommenden Interessen gegen die Geheimhaltungsinteressen abzuwägen, wobei die Ausübung der Meinungsäußerungsfreiheit ausdrücklich genannt wird.

Die Vorgehensweise bei der erforderlichen Interessenabwägung ergibt sich grundsätzlich schon aus dem Erfordernis der verfassungskonformen Anwendung des Informationszugangsrechts gemäß den Vorgaben des Art. 10 EMRK und der dazu ergangenen Rechtsprechung des EGMR, des Verwaltungsgerichtshofes (vgl. grundlegend VwGH 24.5.2018, Ro 2017/07/0026 und VwGH 29.5.2018, Ra 2017/03/0083) und des Verfassungsgerichtshofes (vgl. VfSlg. 20.446/2021).

Welche Interessen abzuwägen sind, ist von den im Einzelfall betroffenen Schutzgütern abhängig; diese sollen alle in die Abwägungsentscheidung einfließen. Eine grundrechtskonforme Abwägung hat sich am sogenannten ***„harm test"*** zu orientieren. Dabei ist zu prüfen, welcher **tatsächliche Schaden** bzw. welche **negativen Auswirkungen** einem legitimen Schutzgut durch die Informationserteilung oder -veröffentlichung drohen würden. Mittels ***„public interest test"*** ist ergänzend zu prüfen, ob ein **überwiegendes öffentliches Interesse** anzunehmen ist, das im Ergebnis für das Zugänglichmachen der Information spricht, obwohl ein gerechtfertigter Geheimhaltungszweck dadurch beeinträchtigt werden könnte. Die Abwägungsentscheidung ist hinreichend zu begründen (AB 2420 BlgNR 27. GP 19; siehe auch *Miernicki* in *Miernicki* (Hrsg), IFG - Informationsfreiheitsgesetz (2024) § 6 IFG K72 bis K74).

II. Zu den Geheimhaltungsgründen bezogenen auf Sachverhalt

§ 6 Abs. 1 Z 1 bis 4 IFG nennt als Ausnahmetatbestände bzw. Geheimnisgründe besonders wichtige öffentliche Interessen. Die Geheimhaltung von Information ist jedenfalls dann geboten, wenn öffentliche Interessen, wie etwa zwingende außenpolitische Gründe, die nationale Sicherheit, die umfassende Landesverteidigung und die Aufrechterhaltung von Ruhe und Sicherheit dies erfordern.

Gerade unter den laut Materialien **„besonders wichtigen" Geheimhaltungsinteressen der Z 1 bis 4** kommt es regelmäßig zu Überschneidungen, sohin kann eine Geheimhaltung bestimmter Informationen **gleichzeitig im Interesse der nationalen Sicherheit, der umfassenden Landesverteidigung** sowie der **Aufrechterhaltung der öffentlichen Ordnung und Sicherheit** erforderlich sein.

Die bisher ergangene Judikatur zum (am 31. August 2025 außer Kraft getretenen) Auskunftspflichtgesetz hält fest, dass es das Gebot der Amtsverschwiegenheit inhaltsleer machen würde, würde die Behörde in ihrer Bescheidbegründung den konkreten Sachverhalt darlegen (müssen). Auch ist es nicht erforderlich, dass der geheim zu haltende Sachverhalt auf eine solche Weise individualisiert wird, dass dieser aus der Bescheidbegründung mit Hilfe von dem Auskunftswerber zugänglichen Schlussfolgerungen ermittelt werden kann (VwSlg 19125 A/2015). Bezogen auf die konkret angefragten Informationen lässt sich diese Rechtsprechung sinngemäß auch auf das IFG übertragen: Würde die Behörde die angefragten Informationen, die geheim zu halten sind, auch nur teilweise oder anonymisiert herausgeben (müssen), so würde dies eben den genannten Geheimhaltungsgründen zuwiderlaufen. Umso mehr gilt dies für die Herausgabe aller angefragten Informationen. IdZ ist auch die **jüngste Entscheidung des BVwG vom 20.3.2026, W292 2332129-1/8E**, zu beachten, in welcher das BVwG hinsichtlich der Geheimhaltungsgründe des IFG ausgesprochen hat, dass der *„Begründungsaufwand der Behörde eingeschränkt* [ist], *sofern Interessen der nationalen Sicherheit betroffen sind. Anderenfalls würde der Zweck des Geheimhaltungstatbestands unterlaufen. Eine ausführliche bzw. detaillierte Begründung wäre in solchen Fällen regelmäßig nur möglich, wenn gerade jene Informationen offengelegt würden, die durch den Geheimhaltungstatbestand geschützt werden sollen.*"(BVwG 20.3.2026, W292 2332129-1/8E, S 13, Pkt. 3.1.6.5).

1. Nationale Sicherheit (Z2)

Das **Interesse der nationalen Sicherheit gemäß § 6 Abs. 1 Z 2 IFG** entspricht dem gleichnamigen Geheimhaltungstatbestand in Art. 10 Abs. 2 EMRK (vgl. AB 2420 BlgNr 27. GP 20); ebenso findet sich dieser Ausnahmetatbestand wörtlich im Art. 22a B-VG wieder. Der EGMR gesteht den Mitgliedstaaten bei diesem Geheimhaltungsgrund insofern einen **weiten Gestaltungsspielraum** zu, dass Beschränkungen des Informationsrechts im überwiegenden öffentlichen Interesse, insbesondere zum Schutz der nationalen Sicherheit, grundsätzlich zulässig sind. Der EGMR betont, dass *„... die nationale Sicherheit ein sich wandelnder und kontextabhängiger Begriff ist, ..."* und dass deswegen den Staaten *„bei der Beurteilung, was in ihren Ländern zu einem bestimmten Zeitpunkt ein Risiko für die nationale Sicherheit darstellt, ein weiter Ermessensspielraum ...."* einzuräumen ist. Der EGMR betont gleichzeitig, dass der Geheimhaltungsgrund „im Interesse der nationalen Sicherheit" zurückhaltend anzuwenden und restriktiv auszulegen ist (EGMR 10.10.2007, 69698/10, *Stoll*, Rn 54; EGMR 3.2.2022, 39325/20, *Šeks*, Rn 63f).

Insbesondere zählen zur nationalen Sicherheit der **Schutz der Unabhängigkeit, Integrität** und **Sicherheit des Landes** und seiner **auswärtigen Beziehungen** (EGMR 3.2.2022, 39325/20, *Šeks*, Rn 63f). Auch etwa Informationen über **Sicherheitsüberprüfungen in sensiblen Bereichen** (EGMR 26.3.1987, 9248/81, *Leander*, Rn 66) oder über **geheime Rüstungsprojekte** (EGMR 16.12.1992, 12945/87, *Hadjianastassiou*, Rn 41) dienen dem Schutz der nationalen Sicherheit (*Schneider* in *Schneider* (Hrsg), IFG - Informationsfreiheitsgesetz (2025) § 6 IFG Rn 12). Es ist nicht zwingend davon auszugehen, dass dieser Tatbestand nur dann erfüllt ist, wenn der Bestand Österreichs als Staat oder die territoriale Integrität Österreichs gefährdet wäre oder eine Unterminierung Österreichs durch Einzelpersonen oder Gruppen zu erwarten ist (*Bußjäger* in *Bußjäger/Dworschak*, Informationsfreiheitsgesetz § 6 Rn 4). Dieser Tatbestand ist vielmehr bereits dann erfüllt, wenn Umstände vorliegen, die nicht unbedingt den Staat als solchen bedrohen, aber durchaus einen Angriff auf seine Souveränität darstellen könnten (VfGH 10.6.1998, B2322/97).

Zu den **Beispielen aus der Rechtsprechung des EGMR zur nationalen Sicherheit** zählen etwa Fälle zur **Bekämpfung von Terrorismus und Spionage** und die **Hintanhaltung ernstlicher Unruhen** (EGMR, Fall *Chalal*, ÖJZ 1997, 633, Rz 75; EGMR, Fall *Zana*, ÖJZ 1998, 716, Rz. 55; EGMR, Fall *Klass* ua, EuGRZ 1979, 285, Rz 48 ff) oder jene zur **Hintanhaltung der Gefährdung der territorialen Integrität** (vgl EGMR 30.1.1998, 133/1996/752/951 *United Communist Party of Turkey/TR,* Rn 40 f). Besonders erwähnenswert ist auch die Judikatur zum Schutz der **Geheimhaltung von geheimdienstlichen Tätigkeiten** im Interesse des Funktionierens einer auf dem Grundsatz der Vorherrschaft des Rechts beruhenden demokratischen Gesellschaft (EGMR, *Observer* und *Guardian*, ÖJZ 1992, 278, Rz 57 und 69; EGMR 9.2.1995, 16616/90 *Vereniging Weekblad Bluf!/NL,* Rz 36; vgl VfGH 21.6.1988, B400/87; VfSlg 11745; *Miernicki*, Zugang zu behördlichen Informationen 260).

Da die nationale Sicherheit **traditionell als Kerngehalt staatlicher Souveränität** anzusehen ist, kann von den zuständigen Behörden kein derartig hohes Maß an detaillierter Begründung erwartet werden, wie dies etwa in anderen Rechtsbereichen (so beispielsweise im Zivil- oder allgemeinem Verwaltungsrecht) vorgesehen ist. In diesem Sinne kann etwa eine detaillierte Begründung, warum ein **Geheimdokument nicht deklassifiziert** werden kann, dem **Zweck der Geheimhaltung bzw. der Klassifizierung entgegenlaufen** (EGMR 3.2.2022, 39325/20, *Šeks*, Rn 71) und letztlich einer **Preisgabe nahekommen** (s. *Koppensteiner/Lehne/Lehofer*, IFG § 6 Rz 10).

Unter den Geheimhaltungsgrund der nationalen Sicherheit sind der **Staats- und Verfassungsschutz** bzw. in diesem Bereich erlangte **nachrichtendienstliche Informationen**, der **Schutz der verfassungsmäßigen Einrichtungen, der Bevölkerung** sowie der wesentlichen **Sicherheitsinteressen der Republik Österreich** vor inneren oder äußeren Bedrohungen zu subsumieren. Darüber hinaus steht die nationale Sicherheit in einem engem Zusammenhang mit dem strafrechtlichen Begriff des „Staatsgeheimnisses".

Unter „Staatsgeheimnis" sind geheime Tatsachen, Erkenntnisse, und Gegenstände zu verstehen, welche vor einer fremden Macht geheim zu halten sind, um die Gefahr eines schweren Nachteils für die Landesverteidigung oder die nationalen Beziehungen Österreichs hintanzuhalten (*Koppensteiner/Lehne/Lehofer*, IFG § 6 Rz 11f).

Die Erläuterungen zu den Geheimhaltungstatbeständen der nationalen Sicherheit sowie der öffentlichen Ordnung und Sicherheit (dazu siehe unten Pkt. 3) halten fest, dass „ *Insbesondere Angelegenheiten des Staatsschutzes und des Nachrichtendienstes [...] regelmäßig unter diese Geheimhaltungstatbestände zu subsumieren ...*" sind (ErlRV 2238 BlgNR 27. GP 8). Die Geheimdienstangelegenheiten berühren *„typischerweise (wenn nicht sogar vordergründig) nationale Sicherheitsinteressen ...*" (*Neusiedler*, Zugang zu Geheimdienstinformationen nach dem IFG, ÖJZ 2025/145, 930; EGMR 9.2.1995, 16616/90, *Vereinigung Weekblad Bluf!/Niederlande*, Rn 33 ff).

Für den nachrichtendienstlichen Bereich besonders relevant sind die Bestimmungen des **Informationssicherheitsgesetzes (InfoSiG)**. Während **§ 2 InfoSiG** die **Beschränkung des Zugangs zu klassifizierten Informationen** regelt, statuiert **§ 3 leg. cit. besondere Voraussetzungen für den Zugang** zu solchen Informationen. Das InfoSiG erfasst nur klassifizierte Informationen, die Österreich im Rahmen völkerrechtlicher Regelungen erhalten hat und bezieht sich in § 2 **explizit auf das Geheimhaltungsregime des § 6 IFG** (vgl. *Neusiedler*, Zugang zu Geheimdienstinformationen nach dem IFG ÖJZ 2025/145, 926). Der Systematik des InfoSiG folgt die **Geheimschutzordnung des Bundes (GehSO)**, welche dem Schutz genuin nationaler Staatsgeheimnisse durch Klassifizierung dient (ErlRV 937 BlgNR 27. 23; siehe auch *Lehne*, Zugang zu Informationen und der Schutz von Staats- und Amtsgeheimnissen, REM 27: Informationsfreiheit und Informationszugang zu journalistischen Zwecken, S. 221f).

Die **Geheimschutzvorschrift (GehSchV) – ein Erlass des BMLV –** bezweckt die Sicherstellung berechtigter Geheimhaltungsinteressen, den Schutz von Staatsgeheimnissen und militärischen Geheimnissen sowie die Umsetzung der völkerrechtlichen/internationalen Verpflichtungen Österreichs zur sicheren Verwendung von klassifizierten Informationen im Ressortbereich des BMLV mit Einschluss des ÖBH. Sie beschreibt den Vorgang der Klassifizierung von Informationen und definiert die einzelnen Klassifizierungsstufen, enthält die Aufgaben und den Verantwortungsbereich des Informationssicherheitspersonals und regelt den Umgang mit klassifizierten Informationen, sowohl für den nationalen als auch den internationalen Bereich. Die Neufassung der GehSchV vom 18. September 2025 ist auf der Homepage des BMLV aufrufbar und berücksichtigt insbesondere auch die Bestimmungen des mit 1. September 2025 in Kraft getretenen IFG. Rechtsgrundlagen für die GehSchV sind ua, (aber nicht nur) und insbesondere im gegebenen Zusammenhang Art. 22a Abs. 2 B-VG, InfoSiG sowie IFG. Die GehSchV gilt im gesamten Ressortbereich des BMLV und ist sowohl auf nationale als auch internationale klassifizierte Informationen anzuwenden.

Klassifizierte Informationen sind demnach Informationen, Tatsachen, Gegenstände und Nachrichten (unabhängig von Darstellungsform und Datenträger), die eines besonderen Schutzes gegen Kenntnisnahme und Zugriff durch Unbefugte bedürfen. Die Klassifizierung einer Information ist die Zuordnung einer Klassifizierungsstufe für diese Information. Die Zuordnung einer Klassifizierungsstufe hat unter Abwägung der erforderlichen administrativen und sicherheitsmäßigen Aufwendungen gegenüber dem im Fall einer Preisgabe zu erwartenden Schaden zu erfolgen. Die GehSchV unterscheidet zwischen vier Klassifizierungsstufen: EINGESCHRÄNKT, VERTRAULICH, GEHEIM und STRENG GEHEIM. Ob klassifizierte Informationen von der Informationspflicht nach IFG sowohl von der proaktiven Informationspflicht als auch von der Information auf Antrag ausgenommen sind, ist jeweils im Rahmen der Einzellfallabwägung zu überprüfen.

Die gegenständlich angefragten Informationen betreffen Aspekte, die unmittelbar die nationale Sicherheit berühren. Der Begriff der nationalen Sicherheit versteht die Behörde im Zusammenhang mit der aktuellen weltweiten Sicherheitssituation, wie sie auch im Risikobild 2025 dargestellt wird: *„Die globale Sicherheitslage hat sich in den letzten Jahren deutlich verschärft, geprägt durch eine zunehmende Abkehr von der regelbasierten Weltordnung. Der russische Angriffskrieg gegen die Ukraine steht exemplarisch für diese Entwicklung, ...“* (Risikobild, S 28f). Diese, im Risikobild 2025 dargestellte, prekäre Sicherheitslage hat sich auch im Risikobild 2026 nicht signifikant verändert. Die diesjährige sicherheitspolitische Prognose ist geprägt von *„tiefgreifenden Umbrüchen“* und der *„Zunahme systemischer Ungewissheit“*. Auch die aktuellen Entwicklungen im Nahen Osten, insbesondere im Iran, verschärfen die ohnehin angespannte geopolitische Weltsicherheitslage.

Durch diese zunehmende Verschärfung der Sicherheitslage ist daher aus der Sicht der Behörde auch das Verständnis des Begriffs „nationale Sicherheit“ an die aktuellen Gegebenheiten anzupassen. *„Das internationale System befindet sich in einer tiefgreifenden Umbruchphase. Globale Machtverschiebungen, geoökonomische Fragmentierungen, technologische Disruption und ökologische Stressfaktoren verändern die Grundlagen europäischer Sicherheitspolitik.“*(Risikobild 2026, S. 22). *„Die instabile Sicherheitslage im Umfeld Europas erfordert sowohl von der NATO als auch der EU, sich verstärkt der militärischen Verteidigung zu widmen. Rüstungs- und Verteidigungsanstrengungen Österreichs und seiner Nachbarn stellen daher insbesondere für ausländische militärische Nachrichtendienste lohnende Ziele dar. ... Die Möglichkeiten der österreichischen Spionageabwehr müssen daher den Herausforderungen der nachrichtendienstlichen Zeitenwende umfassend entsprechen.“* (Risikobild 2026, S. 244).

Die umfassende Prüfung hat ergeben, dass die Offenlegung der betreffenden Inhalte **geeignet** wäre, wesentliche Sicherheitsinteressen der Republik Österreich zu gefährden. Insbesondere besteht die konkrete Gefahr, dass durch die Bekanntgabe Rückschlüsse auf sicherheitsrelevante Strukturen, Maßnahmen und Fähigkeiten des ÖBH gezogen werden

könnten. Die Offenlegung der angefragten Informationen würde potentiell die Wirksamkeit von Schutzmechanismen mindern, laufende oder zukünftige sicherheitsrelevante Maßnahmen gefährden und somit die nationale Sicherheit sowie die nationale Verteidigungsfähigkeit beeinträchtigen.

Darüber hinaus könnte die Offenlegung dieser sensiblen Informationen unbefugten Dritten ermöglichen, Schwachstellen aufzuspüren oder sicherheitsrelevante Prozesse gezielt zu umgehen. Dies würde ein nicht hinnehmbares **Risiko** für die Stabilität und Funktionsfähigkeit des ÖBH darstellen.

Die angefragten Informationen würden offenlegen, welcher konkreter Versionen des Betriebssystems des Unternehmens Microsoft bzw. IBM OS/2 sich das ÖBH (eventuell) bedient oder nicht bedient und es würden dadurch Rückschlüsse auf sicherheitsrelevante Abläufe und Entscheidungsgrundlagen zugelassen. Der **Schaden bzw. die negativen Auswirkungen**, die eintreten könnten, würden in der beeinträchtigten Handlungsfähigkeit der Republik Österreich in diesem sensiblen Sicherheitsbereich liegen. Selbst die Information, dass bestimmte Systeme nicht oder nicht mehr im Einsatz sind, stellt einen Vorteil für den/die potentiellen Angreifer dar, da Schwachstellenscans der IKT-Systeme des ÖBH, wie sie durch das militärische Cyberzentrum täglich beobachtet und abgewehrt werden, deutlich zielgerichteter und effizienter werden würden. Daher sind – nach fundierter Einschätzung der zuständigen Fachabteilung – alle Informationen, die technische Details (wie zB. die jeweilige Softwarebezeichnung oder gar die Version), Bestände oder Übersichtsdarstellungen über die IKT-Systeme des ÖBH enthalten, als EINGESCHRÄNKT zu klassifizieren, da sie ihrer Art nach nicht ohne konkrete Gefahr für die Erfüllung einer Aufgabe des ÖBH preisgegeben werden können.

Grundsätzlich ist daher die begehrte Information iSd GehSchV als EINGESCHRÄNKT klassifiziert. Demnach sind Informationen, die als EINGESCHRÄNKT klassifiziert wurden, solche, deren unbefugte Weitergabe den in § 6 Abs. 1 IFG genannten Interessen zuwiderlaufen würde (EGMR 3.2.2022, 39325/20, *Šeks*, Rn 71). Nach sorgfältiger **Abwägung** zwischen dem Interesse an der Erteilung der Informationen und dem Schutz des übergeordneten Sicherheitsinteresses wurde festgestellt, dass im vorliegenden Fall dem Schutz nationaler Sicherheit der Vorzug zu geben ist, da der Schutz der nationalen Sicherheit ein besonders gewichtiges Rechtsgut darstellt, dessen Beeinträchtigung jedenfalls zu vermeiden ist.

Die Offenlegung der angefragten Informationen würde somit eine erhebliche Gefährdung der **Informations-, Kommunikations- und Führungsfähigkeit** des ÖBH darstellen und ist daher aus Gründen der **nationalen Sicherheit unzulässig.**

2. Umfassende Landesverteidigung (Z3)

Auch das Interesse der **umfassenden Landesverteidigung gemäß § 6 Abs. 1 Z 3 IFG** bildet einen besonders gewichtigen Geheimhaltungsgrund und weist ebenso wie das Interesse der nationalen Sicherheit besondere strafrechtliche und geheimnisschutzrechtliche Bezüge auf (vgl. *Koppensteiner/Lehne/Lehofer*, IFG § 6 Rz 10), die eine Geheimhaltung betroffener Informationen zu rechtfertigen vermag. Auch dieser Geheimhaltungstatbestand findet sich im Art. 22a Abs. 2 B-VG wörtlich wieder. Dieser Geheimhaltungstatbestand umfasst etwa militärische Beschaffungen, Einsatzpläne des Bundesheeres, sonstige Militärgeheimnisse, etwa zu Waffensystemen oder militärischen Übungen (*Miernicki*, Zugang zu behördlichen Informationen 70; EGMR 16.12.1992, 12945/87, *Hadjianastassiou*; EGMR 22.10.2009, 69519/01, *Pasko/RU*).

Aufgabe der umfassenden Landesverteidigung nach **Art. 9a Abs. 1 B-VG** ist es, die **Unabhängigkeit nach außen** sowie die **Unverletzlichkeit und Einheit des Bundesgebietes** zu bewahren, insbesondere zur **Aufrechterhaltung und Verteidigung der immerwährenden Neutralität.** Hierbei sind auch die verfassungsmäßigen Einrichtungen und ihre Handlungsfähigkeit sowie die demokratischen Freiheiten der Einwohner vor gewaltsamen Angriffen von außen zu schützen und zu verteidigen (*Schneider* in *Schneider* (Hrsg), IFG - Informationsfreiheitsgesetz (2025) § 6 IFG Rn 13).

Zur umfassenden Landesverteidigung zählen gemäß **Art. 9a Abs. 2 B-VG** die **militärische Landesverteidigung**, welche dem Bundesheer obliegt und den militärischen Schutz von Neutralität und Souveränität beinhaltet; die **zivile Landesverteidigung**, welche Schutzmaßnahmen für die Zivilbevölkerung und die kritische Infrastruktur vorsieht; die **geistige Landesverteidigung**, welche die Maßnahmen zur Förderung und Erhaltung des Wehrwillens der Bevölkerung beinhaltet sowie die **wirtschaftliche Landesverteidigung**, welche ökonomische Störungen vermeiden und Vorsorgen zur Sicherung der Erhaltung der Leistungsfähigkeit der österreichischen Wirtschaft treffen soll (*Neisser* in *Kneihs/Lienbacher* (Hrsg), Art 9a B-VG, Rz 9 ff).

Ressortspezifisch hat die **militärische Landesverteidigung** iSd **§ 2 Abs. 1 lit. a des Wehrgesetzes 2001 (WG 2001)** die Erfüllung der wesentlichen Aufgaben der umfassenden Landesverteidigung mit militärischen Mitteln sicherzustellen.

Umfasst sind der **militärische Schutz der staatlichen Souveränität und der Neutralität**, Maßnahmen gegen kriegsbedingte Störungen der Wirtschaft, die Vorsorge zum Schutz der Zivilbevölkerung und zum Schutz lebenswichtiger Einrichtungen zur **Aufrechterhaltung der Funktionsfähigkeit der Behörden** (vgl. *Miernicki* in *Miernicki (Hrsg)*, IFG - Informationsfreiheitsgesetz (2024) § 6 IFG Rz K14; *Miernicki*, Zugang zu behördlichen Informationen 70; *Perthold-Stoitzner*, Auskunftspflicht[2], 157; *Wieser* in *Korinek/Holoubek* B-VG Art 20/3, Rz 27), **Schutz der Truppen, Systeme und Einrichtungen des Bundesheeres, Sicherung der**

Einsatz- und Führungsfähigkeit in Krisen- und Verteidigungsfällen, Verhinderung von Spionage, Sabotage und Cyberangriffen sowie die Gewährleistung der **Handlungsfreiheit** staatlicher Organe bei Krisen und Einsätzen.

Dem Geheimhaltungstatbestand der umfassenden Landesverteidigung obliegt der Schutz von Militärgeheimnissen (*Miernicki in Miernicki (Hrsg), IFG - Informationsfreiheitsgesetz (2024)* § 6 IFG K15; *Schneider* in *Schneider* (Hrsg), IFG - Informationsfreiheitsgesetz (2025) § 6 IFG Rz 15). Nach den Begriffsbestimmungen des **§ 1 Abs. 5 des Militärbefugnisgesetzes (MBG)** sind unter **militärischen Geheimnissen** alle militärisch bedeutsamen Tatsachen, Erkenntnisse, Nachrichten und Vorhaben, die nur einem begrenzten Personenkreis zugänglich sind und ihrer Art nach offenbar nicht ohne Gefahr für die Erfüllung einer Aufgabe des Bundesheeres preisgegeben werden können, zu verstehen. Neben militärischen Bereichen und Heeresgut zählen auch militärische Geheimnisse gemäß **§ 1 Abs. 7 Z 3 MBG** zu den **militärischen Rechtsgütern.**

Unter **militärischer Sicherheit ist gemäß § 1 Abs. 11 MBG** der Schutzzustand militärischer Rechtsgüter, der der Art und Schutzwürdigkeit dieser Rechtsgüter sowie der Art und Intensität einer möglichen Gefährdung entspricht, zu verstehen.

Ein Angriff gegen **militärische Rechtsgüter iSv § 1 Abs. 8 MBG** ist die Bedrohung eines geschützten Rechtsgutes durch die rechtswidrige Verwirklichung des Tatbestandes einer gerichtlich strafbaren Handlung, die nicht bloß auf Begehren eines Beteiligten verfolgt wird.

Demnach ist die **Offenlegung von Geheiminformationen** über das ÖBH, wenn dadurch die Verteidigungsbereitschaft betroffen ist, **jedenfalls unzulässig** (vgl. *Koppensteiner/Lehne/Lehofer*, § 6 IFG Rz 13; *Miernicki* in *Miernicki* (Hrsg), IFG - Informationsfreiheitsgesetz (2024) § 6 IFG K15). Dazu gehören etwa Einsatzpläne, Übungs- (EGMR 22.10.2009, 69519/01, *Pasko/RU,* Rz 85 ff) und Truppenpläne oder Details zu spezifischen Waffensystemen (EGMR 16.12.1992, 12945/87, *Hadjianastassiou/GR,* Rz 45 ff).

Die angefragten Informationen stehen in einem unmittelbaren Zusammenhang mit Maßnahmen, Strukturen oder Planungen, die der Sicherstellung der militärischen, zivilen und wirtschaftlichen Verteidigungsfähigkeit der Republik Österreich dienen. Eine Offenlegung der begehrten Informationen könnte Rückschlüsse auf strategische Konzepte, organisatorische Abläufe oder sicherheitsrelevante Ressourcen zulassen und damit die Funktionsfähigkeit entsprechender Vorsorge- und Abwehrmechanismen schwächen.
Insbesondere besteht das Risiko, dass durch die Offenlegung potentielle Schwachstellen identifiziert werden oder bestehende Schutzmechanismen umgangen werden könnten. Dies würde die Fähigkeit der Behörde bzw. des ÖBH beeinträchtigen, auf Krisen, Bedrohungen oder Verteidigungsfälle wirksam zu reagieren.

Grundsätzlich würde jede verfügbare Information über die in den IKT-Systemen des ÖBH eingesetzte Hard- oder Software die feindlichen Akteure im Cyberraum begünstigen und damit die Fähigkeit des ÖBH zum militärischen Eigenschutz erheblich schwächen. Die IKT-Systeme des ÖBH umfassen auch etwa Aufklärungs-, Führungsinformations- und Waffensysteme. Informationen darüber würden nicht nur Rückschlüsse auf die Fähigkeiten und mögliche Einsatzarten ermöglichen, sondern auch Cyber-Angriffe (Sabotage) auf diese Systeme begünstigen. Darüber hinaus sind bereits verschiedene Informationen idZ öffentlich benannt, wie etwa dass das ÖBH aus Gründen der Stärkung der digitalen Souveränität sowie der Verbesserung der Resilienz der Systeme auf das Open Source Office-Produkt „Libre Office" umgestiegen ist. IdZ ist auch die **jüngste Entscheidung des BVwG vom 20.3.2026, W292 2332129-1/8E**, zu berücksichtigen, in welcher das BVwG hinsichtlich der Geheimhaltungsgründe des IFG ausgesprochen hat, dass – obwohl bereits allgemeine Informationen öffentlich sind – *eine* [...] *Offenlegung nichts an der fortbestehenden Schutzbedürftigkeit von Detailinformationen ...*" zu ändern vermag. Das BVwG stellte in dieser Entscheidung klar, dass von der Behörde keine weitergehende Begründung verlangt werden kann, da eine solche zwangsläufig mit einer Preisgabe jener Informationen einhergehen würde, die gerade geheim zu halten sind (BVwG 20.3.2026, W292 2332129-1/8E, S 13, Pkt. 3.1.6.6).

Die gegenständlich angefragten Informationen betreffen Betriebssysteme, die durch den Hersteller nicht mehr gewartet werden und dadurch dramatische Sicherheitslücken aufweisen. Selbst die Information, dass bestimmte Systeme nicht oder nicht mehr im Einsatz sind, stellt einen Vorteil für den potentiellen Angreifer dar, da Schwachstellenscans der IKT-Systeme des ÖBH, wie sie durch das Militärische Cyberzentrum täglich beobachtet und abgewehrt werden, deutlich zielgerichteter und effizienter werden würden. IdZ ist auch auf den Cybersicherheitsbericht 2024 Bedacht zu nehmen, welcher – zusammengefasst – darauf hinweist, dass 2024 ein deutlicher Anstieg der Cyberkriegsaktivitäten verzeichnet wurde, der durch geopolitische Spannungen, die steigende Raffinesse von Cyberangriffen und die Integration von neuen Technologien in Cyber-Operationen bedingt ist (Cybersicherheitsbericht 2024, S 26).

Informationen über die Verwendung bestimmter Betriebssysteme stellen ein **schützenswertes militärisches Rechtsgut** dar und sind aus diesem Grund nicht zugänglich zu machen, da die Bekanntgabe eine Erhöhung von potentiellen Cyberangriffen herbeiführen könnte und dies eine **massive Bedrohung der ressorteigenen Informations- und IKT-Sicherheit** befürchten ließe. Des Weiteren lassen sich aus einer derartigen Informationserteilung Rückschlüsse auf die potentiellen Größen und Strukturen von Organisationen ziehen.

Diese Informationen könnten ua. für **Cyberangriffe fremder Nachrichtendienste oder krimineller Organisationen** und dergleichen gegen das ÖBH verwendet werden. In

unsicheren Zeiten, die von Krieg und Konflikt weltweit geprägt sind, richten Nachrichtendienste ihren Schwerpunkt verstärkt auf Informationen von taktischer und militärischer Relevanz, insbesondere auch bezogen auf militärische Technologie, Forschungs- und Entwicklungsprojekte. Auch der geplante Aufbauplan „Österreichisches Bundesheer 2032+" konnte das Interesse ausländischer Nachrichtendienste nach sich ziehen und so potentiell die Gefahr erhöhen. Geheimhaltungsmaßnahmen im Rahmen der Landesverteidigung sind vor dem Hintergrund der **Vertrauensbildung gegenüber Partnern** sowie der **Minimierung von Informationsrisiken** zu betrachten. Die Glaubwürdigkeit Österreichs und seiner Streitkräfte hängt wesentlich davon ab, dass sicherheitsrelevante Informationen zurückhaltend behandelt werden und keine unnötigen Einblicke in operative oder strategische Planungen an andere Nachrichtendienste gegeben werden (Risikobild 2026, S 244 ff).

Im Rahmen der erforderlichen **Interessenabwägung** zwischen dem Recht auf Informationszugang und dem Erfordernis der umfassenden Landesverteidigung, insbesondere der militärischen Landesverteidigung, wurde festgestellt, dass im vorliegenden Fall das Schutzgut der umfassenden Landesverteidigung schwerer wiegt, da die Sicherstellung der Verteidigungsfähigkeit des Staates ein überragendes öffentliches Interesse darstellt, dessen Gefährdung unbedingt zu vermeiden ist.

3. Öffentliche Ordnung und Sicherheit (Z4)

§ 6 Abs. 1 Z 4 IFG normiert das **Interesse der Aufrechterhaltung der öffentlichen Ordnung und Sicherheit** als weiteren Geheimhaltungsgrund, dessen Schutzgut weitgehend dem in **Art. 10 Abs. 2 EMRK** genannten Ziel der Verhinderung von Störungen der öffentlichen Ordnung entspricht.
Unter diesen Geheimhaltungstatbestand fallen die Gefahrenabwehr iSd **Verbrechensverhütung** und der **vorbeugende Schutz von Rechtsgütern**, der **notwendige Schutz von Einrichtungen der Daseinsvorsorge und kritischen Infrastruktur,** Angelegenheiten des **Staatsschutzes** und des **Nachrichtendienstes** sowie vom Bundeskriminalamt zu besorgende **besonders sensible Angelegenheiten** (zB. Zeugen- oder Opferschutz). Auch im Rahmen der außenwirtschaftsrechtlichen Exportkontrolle kann das Interesse der Aufrechterhaltung der öffentlichen Ordnung und Sicherheit (zB betreffend den Verkehr mit Verteidigungsgütern) maßgeblich sein (AB 2420 BlgNR 27. GP 20).

Nach *Miernicki* ist unter diesen Geheimhaltungsgrund auch die **Herausgabe des Quellcodes von Software** zu subsumieren, da mit Herausgabe des ganzen oder auch nur Teilen des Codes **Schwachstellen ermittelt und ausgenutzt** werden könnten. Ebenso wären auch **Alarmpläne, Einsatztaktiken und Einsatzplanungen**, zB. in Bezug auf Versammlungen oder Veranstaltungen, der Sicherheitsbehörden von diesem Geheimhaltungsgrund umfasst, da bei Herausgabe diese unterlaufen werden könnten (vgl. *Miernicki* in *Miernicki* (Hrsg), IFG - Informationsfreiheitsgesetz (2024) § 6 IFG Rz K18f).

Zu den besonders schutzwürdigen Rechtsgütern zählen gemäß **§ 22 Abs. 1 Z 6 Sicherheitspolizeigesetz (SPG)** Einrichtungen, Anlagen, Systeme oder Teile davon, die eine wesentliche Bedeutung für die Aufrechterhaltung der öffentlichen Sicherheit, die **Funktionsfähigkeit öffentlicher Informations- und Kommunikationstechnologie**, die Verhütung oder Bekämpfung von Katastrophen, den öffentlichen Gesundheitsdienst, die öffentliche Versorgung mit Wasser, Energie sowie lebenswichtigen Gütern oder den öffentlichen Verkehr haben **(kritische Infrastrukturen)**.

Die durchgeführte Prüfung hat ergeben, dass eine Offenlegung der begehrten Informationen geeignet wäre, die öffentliche Ordnung und Sicherheit zu beeinträchtigen. Die angefragten Informationen betreffen Sachverhalte, deren Bekanntgabe geeignet wäre, sicherheitsrelevante Abläufe oder Schutzmaßnahmen offenzulegen. Dies würde das Risiko erhöhen, dass diese Informationen missbräuchlich verwendet werden könnten, um Störungen der öffentlichen Ordnung und Sicherheit herbeizuführen oder sicherheitsrelevante Einrichtungen und Abläufe gezielt zu beeinträchtigen.

Insbesondere könnte die Offenlegung dazu führen, dass potentielle Störer oder unbefugte Dritte Kenntnisse erlangen, die ihnen die Umgehung bestehender Sicherheitsvorkehrungen erleichtern und die Planung bzw. Durchführung ordnungswidriger oder strafbarer Handlungen begünstigen. Dies würde die Fähigkeit der zuständigen Organe beeinträchtigen, die Bevölkerung sowie die kritische Infrastruktur davor zu schützen.

Im Rahmen der gebotenen Interessenabwägung zwischen dem Recht auf Informationszugang und dem Schutz der öffentlichen Ordnung und Sicherheit wurde festgestellt, dass im vorliegenden Fall dem Schutzgut der öffentlichen Ordnung und Sicherheit der Vorzug zu geben ist, da die Gewährleistung eines sicheren und geordneten Zusammenlebens sowie der Schutz von Leben, Gesundheit etc. besonders gewichtige öffentliche Interessen darstellt.

Aus den vorstehenden Ausführungen ergibt sich, dass das BMLV ist als Betreiber **kritischer Infrastruktur** im Sinne des **InfoSiG** und der **Österreichischen Sicherheitsstrategie** verpflichtet, technische Details seiner Systeme nur in dem Maß offenzulegen, wie es für den Betrieb oder gesetzliche Anforderungen erforderlich ist.
Die Offenlegung der angefragten Informationen würde diesen Schutzgrundsätzen widersprechen und könnte die Sicherheit der **militärischen Kommunikations- und Führungsnetze** nachhaltig beeinträchtigen.
Daher ist der Zugang zu diesen Informationen auch **im Interesse der öffentlichen Ordnung und Sicherheit gemäß § 6 Abs. 1 Z 4 IFG zu verwehren**.

III. Verhältnismäßigkeitsprüfung

Beschränkungen und Eingriffe in Grundrechte müssen **verhältnismäßig** sein, dh der mit dem Grundrechtseingriff verfolgte Ziel darf nicht außer Verhältnis zum damit verbundenen Eingriff in das Grundrecht sein. Die Behörde hat das Interesse an der Erteilung der begehrten Information und das Geheimhaltungsinteresse gegeneinander abzuwägen, somit zu prüfen, ob die Geheimhaltung der begehrten Information einen **verhältnismäßigen Eingriff in das Grundrecht auf Informationszugang** darstellt:

Die oben angeführten Ausnahmetatbestände iSd § 6 IFG sind Geheimhaltungsgründe im **öffentlichen Interesse** (*Moick/Slunsky/Kallinger*, IFG, Rz 4.154), sind somit **legitime Ziele** iSd EMRK.

Die Geheimhaltung der begehrten Informationen ist **geeignet (tauglich)**, um die im öffentlichen Interesse liegenden legitimen Ziele zu erreichen, daher nationale Sicherheit, die umfassende Landesverteidigung sowie die öffentliche Ordnung und Sicherheit zu wahren (siehe auch an entsprechender Stelle oben, Pkt. II. Pkt. 1. 2. und 3.).

Die Geheimhaltung der angeforderten Unterlagen ist nach Ansicht der Behörde auch **erforderlich (notwendig)**, um die legitimen Ziele zu erreichen. Dabei wurden Alternativen berücksichtigt (VfSlg 17.817/2006). Die Behörde hat geprüft, ob eine teilweise Offenlegung der angeforderten Unterlagen etwa durch Schwärzung oder Anonymisierung sensibler Passagen möglich wäre. Dabei wurde festgestellt, dass jedwede Informationserteilung zu den angefragten Informationen den oben erörterten Geheimhaltungsgründen zuwiderlaufen würde und sie inhaltsleer machen würde. Darüber hinaus ist nicht auszuschließen, dass selbst bei einer teilweisen Offenlegung durch die Kombination (iSd „Mosaiktheorie") mit bereits öffentlich bekannten oder anderweitig zugänglichen Informationen Rückschlüsse auf sicherheitsrelevante Inhalte gezogen werden könnten. Aus den genannten Geheimhaltungsgründen ist die erforderliche Sicherheit daher nur durch eine vollständige Zurückhaltung der betreffenden Informationen gewährleistet. Darüber hinaus würde – gerade durch eine Anonymisierung oder Schwärzung der geheimzuhaltenden Informationen – der Sinn und Zweck dieses Informationsbegehrens verfehlt, da gerade dadurch die für Sie - als Informationswerber - angeforderten Informationen keinen Inhalt mehr hätten. Die Materialien zum IFG sehen eine teilweise Informationserteilung ua dann vor, sofern die angefragte Information teilbar ist, die teilweise Informationserteilung möglich ist und kein unverhältnismäßiger Aufwand damit verbunden ist (ErlRV 2238 BlgNR 27. GP 11). Im vorliegenden Fall lässt sich keine sinnvolle Teilung der Information vornehmen, da gerade durch die Teilung (etwa Schwärzung der betreffenden Versions-Bezeichnung) das Informationsbegehren ins Leere geführt wird (*Koppensteiner/Lehne/Lehofer*, IFG § 6 Rz 93).

Zwischen den in Frage stehenden Geheimhaltungsgründen und der durch die Geheimhaltung verkürzten Grundrechtsposition des Rechts auf Informationszugang besteht eine **angemessene (adäquate)** Relation. Bei einer Gesamtabwägung zwischen der Schwere des Eingriffs in das Informationszugangsrecht und dem Gewicht der ihn rechtfertigenden Gründe, überwiegt das öffentliche Interesse an der nationalen Sicherheit, umfassenden Landesverteidigung sowie der Aufrechterhaltung der öffentlichen Ordnung und Sicherheit.

IV. Interessenabwägung zwischen behördlichen Geheimhaltungsinteressen und dem Grundrecht auf Informationszugang (§ 6 Abs. 1 letzter Satz IFG und Art. 10 EMRK)

Gemäß **§ 6 Abs. 1 letzter Satz IFG** sind die hier erläuterten **Geheimhaltungsinteressen der Behörde** gegen Ihr Interesse an der **Informationserteilung und Meinungsäußerungsfreiheit abzuwägen.**

Mittels ***harm test*** ist zu prüfen, welcher tatsächlicher Schaden bzw. welche nachteilige Auswirkung einem legitimen Schutzgut durch die Informationserteilung droht. Auf die diesbezüglich aufgeführten **drohenden Schäden bzw. Nachteile** wurde bereits in den vorstehenden Ausführungen eingegangen (siehe oben Pkt. II Pkt. 1., 2. und 3).

Der **Schaden bzw. die negativen Auswirkungen**, die eintreten könnten, würden in der beeinträchtigten Handlungsfähigkeit der Republik Österreich in diesem sensiblen Sicherheitsbereich liegen. Die angefragten Informationen stehen in einem unmittelbaren Zusammenhang mit Maßnahmen, Strukturen oder Planungen, die der Sicherstellung der militärischen, zivilen und wirtschaftlichen Verteidigungsfähigkeit der Republik Österreich dienen. Eine Offenlegung der begehrten Informationen könnte Rückschlüsse auf strategische Konzepte, organisatorische Abläufe oder sicherheitsrelevante Ressourcen zulassen und damit die Funktionsfähigkeit entsprechender Vorsorge- und Abwehrmechanismen schwächen. Insbesondere besteht auch das Risiko, dass durch die Offenlegung potentielle Schwachstellen identifiziert werden oder bestehende Schutzmechanismen umgangen werden könnten. Dies würde die Fähigkeit der Behörde bzw. des ÖBH beeinträchtigen, auf Krisen, Bedrohungen oder Verteidigungsfälle wirksam zu reagieren. Auch das Risiko einer missbräuchlichen Verwendung dieser sensiblen Informationen sowie einer gezielten Beeinträchtigung sicherheitsrelevanter Einrichtungen und Abläufe wäre erhöht sowie auch die Aufrechterhaltung der öffentlichen Ordnung und Sicherheit gefährdet. Insbesondere könnte die Offenlegung dazu führen, dass potentielle Störer oder unbefugte Dritte Kenntnisse erlangen, die ihnen die Umgehung bestehender Sicherheitsvorkehrungen erleichtern und die Planung bzw. Durchführung ordnungswidriger oder strafbarer Handlungen begünstigen. Dies würde die staatliche

Fähigkeit beeinträchtigen, die Bevölkerung sowie die kritische Infrastruktur davor zu schützen.

Mit dem sogenannten ***public interest test*** ist zu prüfen, ob ein überwiegendes öffentliches Interesse anzunehmen ist, das es rechtfertigt, dass trotz Bestehens eines gerechtfertigten Geheimhaltungsinteresses, das durch die Informationserteilung beeinträchtigt wird, die Information dennoch zu erteilen ist. Die Materialien nennen hier exemplarisch Fälle von Korruption (ErlRV 2238 BlgNR 27. GP 8).

Es gilt zu beachten, dass - je höher das öffentliche Interesse an der begehrten Information ist und je wahrscheinlicher es ist, dass aufgrund der Rolle des Informationswerbers als public bzw. social watchdog, die breite Öffentlichkeit erreicht wird und ein Forum für eine öffentliche Debatte geschaffen wird - desto weniger Gewicht den negativen Auswirkungen auf die Geheimhaltungsinteressen zukommt (*Koppensteiner/Lehne/Lehofer*, IFG § 6 Rz 88).

In diesem Zusammenhang kommt insbesondere den ***public bzw. social watchdogs*** eine besondere Rolle bei der Interessenabwägung zu. Mit Ihrem Schreiben vom 1. März 2026, das Sie über die Plattform „FragdenStaat" hochgeladen haben, haben Sie einen Antrag auf Informationserteilung gestellt; auf eine etwaige Rolle als public bzw. social watchdog haben Sie nicht verwiesen, weshalb von der Annahme einer solchen Rolle Abstand genommen wurde und schon aus diesem Grund ist festzuhalten, dass den vom **EGMR aufgestellten Prüfkriterien** (iS EGMR 8.11.2016, 18030/11, *Magyar Helsinki Bizottság/Ungarn, Rz* 157ff; darauf bezugnehmend auch VwGH 29.5.20218, Ra 2017/03/0083), welche **kumulativ** vorliegen müssen, nicht genüge getan wurde.

Angesichts der Schwere der drohenden Schäden bzw. drohenden Nachteile, die einer Herausgabe der begehrten Informationen mit sich bringen würde, die insbesondere die nationale Sicherheit und die umfassende Landesverteidigung der Republik Österreich betreffen und ernsthaft gefährden könnten, ist nicht von einem überwiegenden öffentlichen Interesse auszugehen, welches die Offenlegung der begehren Informationen rechtfertigen würde.

Jedwede Informationserteilung würde Rückschlüsse auf die geheim zu haltenden Informationen zuließen. Schließlich sind diese Informationen nicht einzeln zu betrachten. Bei einer **Gesamtschau** aller bereits bekannter Informationen, etwa aus verschiedenen Medien, könnte es zu einer weitgehenden, wenn auch ungewollten, Zugänglichmachung der Informationen und durch deren Zusammenfügen zu einem Gesamtbild kommen.

Während das Prinzip der Transparenz bei staatlichen Informationen grundsätzlich geboten ist, überwiegt im Fall militärischer und hochsensibler Sicherheitsinformationen iS Verwendung bestimmter IT-Strukturen das **übergeordnete Sicherheitsinteresse der Republik Österreich**.

Die begehrte Informationserteilung hätte **keinen Mehrwert für die Öffentlichkeit**, würde aber die **Angriffsfläche** und das **Sicherheitsrisiko** signifikant erhöhen, weshalb die **Geheimhaltung** im **Interesse der nationalen Sicherheit, der umfassenden (insbesondere militärischen) Landesverteidigung** sowie der **Aufrechterhaltung der öffentlichen Ordnung und Sicherheit** jedenfalls als **tauglich, erforderlich und verhältnismäßig** anzusehen ist.

Es war daher spruchgemäß zu entscheiden.

RECHTSMITTELBELEHRUNG

Gegen diesen Bescheid ist das Rechtsmittel der Beschwerde an das Bundesverwaltungsgericht zulässig. Sie hat den angefochtenen Bescheid und die Behörde, die den Bescheid erlassen hat, zu bezeichnen. Weiters hat die Beschwerde die Gründe, auf die sich die Behauptung der Rechtswidrigkeit stützt, ein bestimmtes Begehren und die Angaben, die erforderlich sind, um zu beurteilen, ob die Beschwerde rechtzeitig eingebracht wurde, zu enthalten. Die Beschwerde ist schriftlich innerhalb von 4 Wochen ab Zustellung des Bescheides beim Bundesministerium für Landesverteidigung, Roßauer Lände 1, 1090 Wien einzubringen.

Eine rechtzeitig eingebrachte und zulässige Beschwerde hat aufschiebende Wirkung, das heißt, der Bescheid kann bis zur abschließenden Entscheidung nicht vollstreckt werden.

Bis zur Vorlage der Beschwerde an das Bundesverwaltungsgericht sind die Schriftsätze bei der belangten Behörde einzubringen.

Eine Beschwerde ist nicht mehr zulässig, wenn die Partei nach der Zustellung oder Verkündung des Bescheides ausdrücklich auf die Beschwerde verzichtet hat.

HINWEIS

Nach § 1 der Verordnung des Bundesministers für Finanzen betreffend die Gebühr für Eingaben bei den Verwaltungsgerichten (VwG-Eingabengebührverordnung – VwG-EGebV), BGBl. II Nr. 387/2014, unterliegen Eingaben und Beilagen an die Verwaltungsgerichte einer Pauschalgebühr nach dieser Verordnung, soweit nicht gesetzlich Gebührenfreiheit vorgesehen ist.

Die Gebührenschuld für die Eingaben und Beilagen entsteht im Zeitpunkt der Einbringung der Eingabe; erfolgt die Einbringung jedoch im Wege des elektronischen Rechtsverkehrs,

entsteht die Gebührenschuld, wenn ihre Daten zur Gänze bei der Bundesrechenzentrum GmbH eingelangt sind. Mit dem Entstehen der Gebührenschuld wird die Gebühr fällig.

Nach § 2 Abs. 1 Z 1 und 2 VwG-EGebV beträgt die Pauschalgebühr für Beschwerden, Wiedereinsetzungsanträge, Wiederaufnahmeanträge und sonstige das Verfahren einleitende Anträge 50 Euro sowie für Vorlageanträge, Anträge auf Bewilligung der Verfahrenshilfe oder von einer Beschwerde gesondert eingebrachte Anträge auf Ausschluss oder Zuerkennung der aufschiebenden Wirkung einer Beschwerde 25 Euro.

Beilagen und sonstige nicht in § 2 Abs. 1 VwG-EGebV genannte Eingaben werden durch die Pauschalgebühren des § 2 Abs. 1 VwG-EGebV abgegolten und unterliegen keiner Gebührenpflicht nach dem Gebührengesetz 1957 oder dieser Verordnung.

Die Gebühr ist unter Angabe des Verwendungszwecks auf das Konto des Finanzamtes Österreich, IBAN: AT83 0100 0000 0550 4109, BIC: BUNDATWW, zu entrichten.

Die Entrichtung der Gebühr ist durch einen Zahlungsbeleg oder einen Ausdruck über die erfolgte Erteilung einer Zahlungsanweisung nachzuweisen.

Dieser Beleg ist der Eingabe anzuschließen. Für jede Eingabe ist die Vorlage eines gesonderten Beleges erforderlich.

Wird eine Eingabe im Weg des elektronischen Rechtsverkehrs eingebracht und besteht eine Schnittstelle zwischen Finanzamt Österreich und dem Verwaltungsgericht, ist die Gebühr durch Abbuchung und Einziehung zu entrichten. In der Eingabe ist das Konto, von dem die Gebühr einzuziehen ist, oder der Anschriftcode (§ 21 Abs. 3 des Bundesverwaltungsgerichtsgesetzes, BGBl. I Nr. 10/2013 in der geltenden Fassung), unter dem ein Konto gespeichert ist, von dem die Gebühr eingezogen werden soll, anzugeben.

Die Stelle, bei der eine Eingabe eingebracht wird, die nicht oder nicht ausreichend vergebührt wurde, hat gemäß § 34 Abs. 1 des Gebührengesetzes 1957 das Finanzamt Österreich darüber in Kenntnis zu setzen.

WIEN, am 12.05.2026
Für die Bundesministerin:

[redacted]

Elektronisch gefertigt

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR LANDESVERTEIDIGUNG @ AMTSSIGNATUR	**Unterzeichner**	Bundesministerium für Landesverteidigung
	Datum/Zeit-UTC	2026-05-12T11:52:16+02:00
	Prüfinformation	Informationen zur Prüfung der elektronischen Signatur bzw. des Ausdrucks finden Sie unter: http://www.bmlv.gv.at/amtssignatur
Hinweis	Dieses Dokument wurde amtssigniert. Auch ein Ausdruck dieses Dokuments hat gemäß § 20 E-Government-Gesetz die Beweiskraft einer öffentlichen Urkunde.	