Bundesministerium
Landesverteidigung

bmlv.gv.at

Abteilung Präsidiale

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

Sebastian PFEIFER
[redacted]

Geschäftszahl: S90620/1493-Präs/BürgSrv/2025 (1)

Bezug
S90620/1245-Präs/BürgSrv/2025

PFEIFER Sebastian;
IP-Ranges im Bundesministerium für Landesverteidigung und dessen nachgeordneten Dienststellen;
Bescheid gemäß § 11 Abs. 1 IFG

B E S C H E I D

Über Ihren Antrag auf bescheidmäßige Erledigung nach § 11 Abs. 1 des Informationsfreiheitsgesetzes (IFG), BGBl. I Nr. 5/2024 zu Ihrem Ersuchen auf Zugang zu Informationen gemäß §§ 7 ff IFG vom 8. September 2025 ergeht von der Bundesministerin für Landesverteidigung als zuständige Behörde folgender

SPRUCH:

Der begehrte Zugang zu Informationen betreffend die IP-Adressbereiche (IP-Ranges) des Bundesministeriums für Landesverteidigung und dessen nachgeordneten Dienststellen wird gemäß Art. 22a Abs. 2 des Bundes-Verfassungsgesetzes (B-VG) iVm § 6 Abs. 1 IFG wegen des Entgegenstehens von Geheimhaltungsgründen **nicht gewährt.**

BEGRÜNDUNG

Mit E-mail vom **8. September 2025** ersuchten Sie gemäß § 7 Abs. 1 IFG um Zugang zu folgenden Informationen:

„Welche IP-Bereiche werden vom Bundesministerium für Landesverteidigung und dessen nachgeordneten Dienststellen, vom BMLV verwalteten oder kontrollierten Fonds, Anstalten, Körperschaften, Einrichtungen oder Unternehmen verwendet bzw. welche IP-Adressen/IP-Bereiche wurden statisch von Internetprovidern den genannten Stellen zugewiesen; Aufgeschlüsselt nach Stelle/Unternehmen?“

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

Aufgrund der Komplexität der Anfrage und der damit verbundenen erforderlichen Abstimmung ressortinterner Fachabteilungen wurde die Beantwortungsfrist gemäß § 8 Abs. 2 IFG um weitere 4 Wochen verlängert, dies wurde Ihnen rechtskonform innerhalb offener Frist gemäß § 8 Abs. 1 IFG per Rsa-Schreiben vom 30. September 2025, GZ S90620/1245-Präs/BürgSrv/2025 (2), mitgeteilt.

Mit Schreiben vom **9. Oktober 2025**, GZ S90620/1245-Präs/BürgSrv/2025(1), erging schließlich die Mitteilung an Sie, dass die begehrte Information wegen des Vorliegens von Geheimhaltungsinteressen nicht erteilt werden könne.

Daraufhin verwiesen Sie in Ihrer E-mail vom **22. Oktober 2025** auf Ihr initial mit der Antragstellung auf Zugang zu Informationen gestelltes Eventualbegehren auf Ausstellung eines Bescheides im Falle der Nichtgewährung des Zuganges zur Information gemäß § 11 Abs. 1 IFG.

Die Behörde hat erwogen:

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 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.

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 **§ 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 ein Bescheid zu erlassen. Als Verfahrensordnung, nach der der Bescheid zu erlassen ist, gilt das AVG, sofern der 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).

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.

In diesem Zusammenhang verweisen die Erläuterungen zum Informationsfreiheitsgesetz auf die Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte (EGMR) zu Art. 10 EMRK „ready and available“ (zB EGMR 14.4.2009, *Társaság a Szabadságjogokért*, BeschwNr. 37374/05, Z 36; EGMR 8.11.2016, *Magyar Helsinki Bizottság*, BeschwNr. 18030/11, Z 169 ff; EGMR 30.1.2020, *Studio Monitori* ua., BeschwNr. 44920/09 ua., Z 39 ff). Der EGMR berücksichtigt bei seiner Schlussfolgerung, ob die Verweigerung des Zugangs zu Informationen eine Verletzung von Art. 10 EMRK darstellt, also stets den Umstand, ob die begehrte Information **vorhanden und verfügbar** ist.

Das Bundesministerium für Landesverteidigung (BMLV) verwendet IP-Adressen aus dem öffentlich - in der RIPE Datenbank abrufbaren — Bereich.

Bezugnehmend auf das weitergehende Informationsersuchen dahingehend, welche IP-Adressen/IP-Bereiche statisch von Internetprovidern den genannten Stellen zugewiesen worden seien bzw. die Darlegung einer entsprechenden Aufschlüsselung nach Stelle/Unternehmen ist darauf zu verweisen, dass sich Informationsbegehren auf bereits bekannte Tatsachen zu beziehen haben, die **nicht erst erhoben, recherchiert, gesondert aufbereitet oder erläutert werden müssen** (vgl. ErlRV 2238 BlgNR 27. GP 6); nicht existente Informationen sind folglich auch nicht „ready and available“.

Da das BMLV über keine Liste der Zuweisungen von IP-Adressen bzw. IP-Bereichen bzw. eine entsprechende Aufschlüsselung nach Stellen/Unternehmen verfügt, ist die Erstellung einer gesonderten Liste bereits aus diesen Gründen nicht vom Anwendungsbereich des IFG umfasst.

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

Verfassungsgesetzliche Geheimhaltungsgründe finden sich in Art. 22a Abs. 2 B-VG. 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 nicht, 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 angeführten Ausnahmetatbestände 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 Geheimhaltungsgrund **„erforderlich und verhältnismäßig“** ist (vgl. *Koppensteiner/Lehne/Lehofer*, IFG § 6 Rz 82). Unter „erforderlich“ ist geboten bzw. „notwendig“ iS der grundrechtlichen Gesetzesvorbehalte der EMRK zu verstehen (s. ErlRV 2238 BlgNR 27. GP 3).

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.

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“).

Sohin ist das gegenständliche Informationsbegehren dahingehend zu prüfen, ob einer Informationserteilung Geheimhaltungsverpflichtungen entgegenstehen.

Die Geheimhaltung von Information ist jedenfalls dann geboten, wenn öffentliche Interessen, wie etwa die **nationale Sicherheit, die umfassende Landesverteidigung und die Aufrechterhaltung von Ruhe und Sicherheit** dies erfordern.

Das **Interesse der nationalen Sicherheit gemäß § 6 Abs. 1 Z 2 IFG** entspricht dem gleichnamigen Geheimnistatbestand in **Art. 10 Abs. 2 EMRK**. 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, betont aber gleichzeitig, dass dieser Geheimhaltungsgrund zurückhaltend anzuwenden und restriktiv auszulegen ist (EGMR 3.2.2022, 39325/20, *Šeks*, Rn 63f); es wird insbesondere ein „erheblicher Grad" der Gefährdung von militärischen Interessen vorausgesetzt (vgl. ErlRV 2238 BlgNR 27. GP 8).

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 Österreichs** (vgl EGMR 30.1.1998, 133/1996/752/951 *United Communist Party of Turkey/TR* Rz 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, Fall *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 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.

Für den Geheimdienstbereich besonders relevant sind die Bestimmungen des **Informationssicherheitsgesetzes (InfoSiG)**. Während **§ 2 InfoSiG** die **Beschränkung des Zugangs zu klassifizierten Informationen** regelt, statuiert **§ 3 InfoSiG 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).

Die IP-Adressbereiche des Bundesministeriums für Landesverteidigung sind Teil der **militärischen Kommunikations- und IT-Infrastruktur** der Republik Österreich. Eine Offenlegung dieser Adressbereiche würde potenziellen Angreifern ermöglichen, gezielte technische Aufklärungsmaßnahmen (z. B. Netzwerkscans, Port-Scans, Schwachstellenanalysen) durchzuführen.

Dies könnte zur **Erkennung, Lokalisierung und Ausnutzung** von Systemen führen, die für die **Einsatzführung, Nachrichtengewinnung, Logistik und Verwaltung** wesentlich sind.

Die Konfigurationen der IKT-Komponenten sind als **"eingeschränkt"** klassifiziert und **daher einer entsprechenden Geheimhaltung** zur **Wahrung der militärischen Handlungsfähigkeit und Einsatzbereitschaft** unterzogen. Die in diesen Konfigurationen enthaltenen IP-Adressen unterliegen derselben Klassifizierungsstufe und können aus diesem Grund nicht zugänglich gemacht werden, darüber hinaus böte die Kenntnis konkreter IP-Adressen die Möglichkeiten von Angriffsvektoren im Cyberraum.

Die Veröffentlichung der IP-Adressbereiche würde somit eine erhebliche Gefährdung der **Informations-, Kommunikations- und Führungsfähigkeit** des Ressorts darstellen und ist daher aus Gründen der **nationalen Sicherheit unzulässig.**

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.

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.

Den Kern der umfassenden Landesverteidigung bildet die **militärische Landesverteidigung iSv § 2 Abs. 1 lit. a des Wehrgesetzes 2001 (WG 2001)**, welche die Erfüllung der Aufgaben der umfassenden Landesverteidigung mit militärischen Mitteln sicherzustellen hat.

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.

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 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 Bundesheer, wenn dadurch die Verteidigungsbereitschaft betroffen ist, **jedenfalls unzulässig** (vgl. *Koppensteiner/Lehne/Lehofer*, § 6 IFG, Rz 13).

Auch Informationen über interne IP-Adressen/Bereiche stellen ein **schützenswertes militärisches Rechtsgut** dar und sind aus diesem Grund nicht zugänglich zu machen, da die Bekanntgabe von IP-Adressen entsprechende Angriffsvektoren eröffnen könnte und dies eine **massive Bedrohung der Informations- und IKT-Sicherheit des Abwehramtes** befürchten ließe. Des weiteren lassen sich aus einer Darstellung von privaten sowie öffentlichen IP-Adressenbereiche Rückschlüsse auf die potentielle Größe und Struktur einer Organisation ziehen.

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

Dies hätte eine massive Gefährdung der **Informations- und Kommunikationssicherheit**, der **Einsatzbereitschaft** des Abwehramts, sowie in **weiterer Folge der militärischen Sicherheit** zur Folge. Die Möglichkeit einer Geolokalisierung würde eine Vorstufe zur Aufklärung von militärischen Liegenschaften und Außenstellen des Abwehramts bilden, was nicht nur eine direkte Bedrohung der militärischen Sicherheit dieser Liegenschaft selbst, sondern eine Möglichkeit der Aufklärung der Angehörigen des Abwehramtes und die **Gefährdung des militärischen Eigenschutzes** darstellen würde.

Eine Geheimhaltung der begehrten Informationen liegt daher j**edenfalls im Interesse der umfassenden Landesverteidigung gemäß § 6 Abs. 1 Z 3 IFG.**

§ 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 (s. ErlRV 2238 BlgNR 27. GP 9).

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 um-

fasst, 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).**

Das BMLV ist als Betreiber **kritischer Infrastruktur** im Sinne des **Informationssicherheitsgesetzes (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 Veröffentlichung der IP-Ranges würde diesen Schutzgrundsätzen widersprechen und könnte die Sicherheit der **gesamten militärischen Kommunikations- und Führungsnetze** 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**.

Während das Prinzip der Transparenz bei staatlichen Informationen grundsätzlich wünschenswert ist, überwiegt im Fall militärischer IT-Strukturen das **übergeordnete Sicherheitsinteresse der Republik Österreich**.

Die Veröffentlichung von IP-Ranges 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 (insb. 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 16.12.2025
Für die Bundesministerin:

[redacted]

Elektronisch gefertigt

Information:

Der Schriftverkehr mit dem Bundesministerium für Landesverteidigung und den Dienststellen des Österreichischen Bundesheeres kann in jeder technisch möglichen Form übermittelt werden, mit E-Mail jedoch nur insoweit, als für den elektronischen Verkehr nicht besondere Übermittlungsformen vorgesehen sind.

Technische Voraussetzungen bzw. Beschränkungen unter https://www.bmlv.gv.at/misc/egovernment/elkomm.shtml

Datenschutzerklärung unter https://www.bundesheer.at/misc/datenschutz.shtml

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR LANDESVERTEIDIGUNG @ AMTSSIGNATUR	**Unterzeichner**	Bundesministerium für Landesverteidigung
	Datum/Zeit-UTC	2025-12-16T14:40:22+01:00
	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.	