

Bundesgesetz über die Umsetzung völkerrechtlicher Verpflichtungen zur sicheren Verwendung von Informationen (Informationssicherheitsgesetz - InfoSiG)

StF: [BGBl. I Nr. 23/2002](#) (NR: GP XXI [RV 753 AB 941 S. 89](#). BR: [AB 6549 S. 683.](#))

Änderung

[BGBl. I Nr. 129/2003](#) (NR: GP XXII [RV 312 AB 322 S. 40](#). BR: [6924 AB 6945 S. 704.](#))

[BGBl. I Nr. 10/2006](#) (NR: GP XXII [RV 1084 AB 1244 S. 129](#). BR: [AB 7449 S. 729.](#))

[BGBl. I Nr. 32/2018](#) (NR: GP XXVI [RV 65 AB 97 S. 21](#). BR: [9947 AB 9956 S. 879.](#)) [CELEX-Nr.: [32016L0680](#)]

[BGBl. I Nr. 50/2025](#) (NR: GP XXVIII [RV 129 AB 151 S. 35](#). BR: [11651 AB 11654 S. 980.](#))

1. Abschnitt

Ziel und Anwendungsbereich des Gesetzes im Bereich der Dienststellen des Bundes

§ 1. (1) Ziel der Bestimmungen der §§ 1 bis 10 ist die Umsetzung völkerrechtlicher Verpflichtungen Österreichs zur sicheren Verwendung von klassifizierten Informationen, unabhängig von Darstellungsform und Datenträger, im Bereich der Dienststellen des Bundes.

(2) Die Voraussetzungen für den Zugang zu klassifizierten Informationen nach § 3 Abs. 1 gelten nicht für den Bundespräsidenten, den Bereich des Nationalrates und des Bundesrates, die Mitglieder der Bundesregierung, die Staatssekretäre, die Gerichtsbarkeit, den Verfassungsgerichtshof und den Verwaltungsgerichtshof, den Rechnungshof und die Volksanwaltschaft. Die Weitergabe von klassifizierten Informationen an diese Organe und Einrichtungen unterliegt keinen Beschränkungen nach diesem Bundesgesetz, jedoch völkerrechtlich vorgesehenen Einschränkungen.

Federal Act on Implementation of Obligations under International Law for Secure Use of Information (Information Security Act, - InfoSiG)

← Original version

as amended by:

(list of amendments published in the Federal Law Gazette [F. L. G. = BGBl.])

← amendment entailing the latest update of the present translation

(the German version is updated to reflect also recent amendments; interim changes are highlighted as **deletions** and **insertions** respectively)

Click [here](#) for checking the up-to-date list of amendments

in the Austrian Legal Information System.

1st Section

Objective and Scope of Application of the Act in the area of the offices of the Federal Government

§ 1. (1) Objective of the regulations of §§ 1 to 10 is to implement obligations of Austria under international law for the secure use of classified information in the area of the offices of the federal government, independent of form of presentation and data storage medium.

(2) The prerequisites for the access to classified information as per § 3 para. 1 do not apply to the Federal President, the area of the National Council and the Federal Council, the members of the Federal Government, the secretaries of state, the courts of law, the Constitutional Court and the Supreme Administrative Court, the Auditor-General's office and the Ombudsmen. The forwarding of classified information to these organs and institutions is not subject to any restrictions according to this federal act, however they are subject to restrictions of international law.

(3) Dieses Bundesgesetz berührt nicht die den in Abs. 2 genannten Organen und Einrichtungen übertragenen Verpflichtungen und Aufgaben.

Beschränkung des Zugangs zu klassifizierten Informationen

§ 2. (1) Der Zugang zu klassifizierten Informationen, die Österreich im Einklang mit völkerrechtlichen Regelungen erhalten hat, ist in dem von den übermittelnden Stellen vorgesehenen Maß und für die von diesen vorgesehene Dauer zu beschränken, wenn dies gemäß ~~Art. 20 Abs. 3 B-VG~~ § 6 Abs. 1 des [Informationsfreiheitsgesetzes – IFG, BGBl. I Nr. 5/2024](#), geboten ist.

(2) Gemäß Abs. 1 erhaltene klassifizierte Informationen sind zur Wahrung des von den übermittelnden Stellen vorgesehenen Schutzes einer der folgenden Klassifizierungsstufen zuzuordnen:

1. „EINGESCHRÄNKT“, wenn die unbefugte Weitergabe der Informationen den in ~~Art. 20 Abs. 3 B-VG~~ § 6 Abs. 1 IFG genannten Interessen zuwiderlaufen würde;
2. „VERTRAULICH“, wenn die Informationen nach anderen Bundesgesetzen unter strafrechtlichem Geheimhaltungsschutz stehen und ihre Geheimhaltung im öffentlichen Interesse gelegen ist;
3. „GEHEIM“, wenn die Informationen vertraulich sind und ihre Preisgabe zudem die Gefahr einer erheblichen Schädigung der in ~~Art. 20 Abs. 3 B-VG~~ § 6 Abs. 1 IFG genannten Interessen schaffen würde;
4. „STRENG GEHEIM“, wenn die Informationen geheim und überdies ihr Bekanntwerden eine schwere Schädigung der in ~~Art. 20 Abs. 3 B-VG~~ § 6 Abs. 1 IFG genannten Interessen wahrscheinlich machen würde.

(3) Solange Informationen klassifiziert sind, findet auf sie § 5 des Bundesarchivgesetzes, BGBl. I Nr. 162/1999, keine Anwendung.

Voraussetzungen für den Zugang zu klassifizierten Informationen

§ 3. (1) Unbeschadet des § 1 darf der Zugang zu klassifizierten Informationen nur unter folgenden Voraussetzungen gewährt werden:

1. einem Bediensteten einer Dienststelle des Bundes, wenn
 - a) der Zugang zu diesen Informationen für die Erfüllung seiner dienstlichen Aufgaben erforderlich ist,
 - b) er nachweislich ausreichend über den Umgang mit klassifizierten Informationen unterwiesen wurde und,

(3) This federal act does not affect the obligations and duties assigned to the organs and institutions mentioned in para. 2.

Restriction of the Access to Classified Information

§ 2. (1) The access to classified information, which Austria has received in accordance with regulations of international law, has to be restricted to the extent and for the duration provided by the originating offices, provided this is required as per Art. 20 para. 3 [Federal Constitutional Law](#).

(2) For maintaining the protection specified by the originating offices, the classified information received as per para. 1 has to be classified in one of the following category levels:

1. "EINGESCHRÄNKT" [RESTRICTED], if the unauthorised disclosure of the information would go directly against the interests mentioned in Art. 20 para. 3 [Federal Constitutional Law](#);
2. "VERTRAULICH" [CONFIDENTIAL], if the information is under a privacy protection of criminal law as per other federal acts and maintaining its secrecy is in the public interest;
3. "GEHEIM" [SECRET], if the information is confidential and moreover its disclosure would create the danger of considerable damage of the interests mentioned in Art. 20 para. 3 [Federal Constitutional Law](#);
4. "STRENG GEHEIM" [TOP SECRET], if the information is secret and moreover its disclosure would probably lead to heavy damage of the interests mentioned in Art. 20 para. 3 [Federal Constitutional Law](#).

(3) As long as information is classified, § 5 of the Federal Archive Act, FLG I no. 162/1999, does not apply.

Prerequisites for the Access to Classified Information

§ 3. (1) Regardless of § 1 the access to classified information may be granted only under the following conditions:

1. a public employee of an office of the federal government, if
 - a) the access to this information is required for the fulfilment of his official duties,
 - b) there is evidence of him being sufficiently instructed about dealing with classified information,

c) soweit Informationen betroffen sind, die als „VERTRAULICH“, „GEHEIM“ oder „STRENG GEHEIM“ klassifiziert wurden, eine Sicherheitsüberprüfung gemäß §§ 55 bis 55b SPG, BGBl. Nr. 566/1991, oder, sofern gesetzlich vorgesehen, eine Verlässlichkeitsprüfung gemäß §§ 23 und 24 MBG, BGBl. I Nr. 86/2000, durchgeführt wurde.

2. sonstigen Personen, wenn

- a) dies für die Ausübung einer im öffentlichen Interesse gelegenen Tätigkeit erforderlich ist,
- b) die Voraussetzungen der Z 1 lit. b und c vorliegen und
- c) kein geringerer als der von der zuständigen Dienststelle vorgesehene Schutzstandard gewährleistet wird.

(2) Ein Bediensteter einer Dienststelle des Bundes darf den Zugang zu klassifizierten Informationen nur unter den Voraussetzungen des Abs. 1 Z 1 suchen.

(Anm.: Abs. 3 aufgehoben durch Art. 3 Z 2, BGBl. I Nr. 32/2018)

Verschwiegenheitspflicht

§ 4. Jede Person, der auf Grund dieses Bundesgesetzes Zugang zu klassifizierten Informationen gewährt wird,

1. ist zur Verschwiegenheit über die ihr dadurch zur Kenntnis gelangten Informationen verpflichtet und
2. hat durch Einhaltung der vorgesehenen Schutzstandards dafür Sorge zu tragen, dass kein Unbefugter Kenntnis von den klassifizierten Informationen erlangt.

Amtshilfe

§ 5. Im Rahmen der Leistung von Amtshilfe dürfen klassifizierte Informationen nur weitergegeben werden, wenn das ersuchende Organ dies ausdrücklich begehrt und den erforderlichen Schutzstandard zu gewährleisten vermag. Im Begehren ist anzugeben, bis zu welcher Klassifizierungsstufe für einen ausreichenden Schutzstandard vorgesorgt ist.

Informationssicherheitsverordnung

§ 6. Die Bundesregierung hat für die Dienststellen des Bundes durch Verordnung Vorschriften über die Informationssicherheit zu erlassen. Diese haben jedenfalls zu regeln:

1. die Kennzeichnung von klassifizierten Informationen,

c) as far as information, which was classified as "CONFIDENTIAL", "SECRET" or "TOP SECRET", is concerned, a security check as per §§ 55 to 55b SPG, FLG no. 566/1991 or, if provided by law, a reliability test as per §§ 23 and 24 MBG, FLG I no. 86/2000 was carried out.

2. other persons, if

- a) this is required for carrying out an activity which is in public interest,
- b) the prerequisites of the points 1 b) and c) apply and
- c) a protection standard not less than that prescribed by the responsible office is ensured.

(2) An employee of an office of the federal government may request access to classified information only under the conditions in para. 1 point 1.

(Note: Para 3 repealed by Art. 3 no. 2, Federal Law Gazette no. 32/2018)

Obligation of Secrecy

§ 4. Any person, to whom access to classified information is granted as per this federal act,

1. is obliged to keep the information he has accordingly received secret and
2. has to ensure by complying to the specified protection standards that no unauthorised person gains knowledge about the classified information.

Administrative Assistance

§ 5. When providing administrative assistance, classified information may only be passed on if the requesting authority particularly requests for it and is able to ensure the required protection standard. The request has to mention up to which classification level a sufficient protection standard is provided for.

Information Security Ordinance

§ 6. The Federal Government must issue regulations about information security for the offices of the federal government through ordinance. They must regulate:

1. The marking of classified information,

2. Maßnahmen und Verhaltensregeln für den Umgang mit klassifizierten Informationen, insbesondere hinsichtlich der Übermittlung, der Vervielfältigung, der Aufbewahrung und der Vernichtung der Informationen,
3. Verhaltensregeln im Fall der Wahrnehmung eines Mangels im Bereich der Informationssicherheit,
4. Zugangsbeschränkungen, die nach Klassifizierungsstufen zu unterscheiden sind,
5. Maßnahmen zur Gewährleistung der Feststellbarkeit des Zugangs zu klassifizierten Informationen,
6. Maßnahmen zur Überprüfung der weiteren Notwendigkeit der Klassifizierung,
7. zu Zwecken der Informationssicherheit erforderliche technische Datensicherheitsmaßnahmen sowie
8. die Vorgangsweise bei der Deklassifizierung von Informationen.

Informationssicherheitsbeauftragte

§ 7. (1) Jeder Bundesminister bestellt für seinen Wirkungsbereich einen Informationssicherheitsbeauftragten und dessen Stellvertreter.

(2) Dem Informationssicherheitsbeauftragten obliegt die Überwachung der Einhaltung der Bestimmungen dieses Bundesgesetzes, der Informationssicherheitsverordnung, der Übereinkommen gemäß § 14 und der sonstigen Informationssicherheitsvorschriften sowie die periodische Überprüfung der Sicherheitsvorkehrungen für den Schutz von klassifizierten Informationen und die Berichterstattung darüber an die Informationssicherheitskommission nach § 8. Im Falle der Wahrnehmung eines Mangels hat der Informationssicherheitsbeauftragte auf die unverzügliche Behebung des Mangels hinzuwirken.

(3) Der Informationssicherheitsbeauftragte trägt dafür Sorge, dass in seinem Ressortbereich alle Personen, auf die die Voraussetzungen des § 3 Abs. 1 Z 1 bis 2 zutreffen, sicherheitsüberprüft werden.

(4) Der Informationssicherheitsbeauftragte hat den zuständigen Bundesminister in Angelegenheiten der Informationssicherheit zu beraten und erforderlichenfalls Vorschläge zu deren Verbesserung zu erstatten.

2. Measures and code of behaviour for dealing with classified information, particularly with regard to the transmission, copying, storage and destruction of the information,
3. Code of behaviour in case of noticing a defect in the area of the information security,
4. Access restrictions to be differentiated according to the classification levels,
5. Measures for ensuring the determination of the access to classified information,
6. Measures for checking further necessity of the classification,
7. Required technical data security procedures for the purpose of information security, as well as
8. The procedure for declassifying information.

Information Security Officer

§ 7. (1) For his sphere of action every Federal Minister appoints an information security officer and his deputy.

(2) The information security officer is responsible for the supervision of the compliance with the regulations of this federal act, the Information Security Ordinance, of the agreements as per §14 and the other information security regulations, as well as the periodical inspection of the security precautions for the protection of classified information and the reporting on this to the Information Security Commission as per § 8. In case of noticing a defect, the information security officer has to work towards immediate removal of the defect.

(3) The information security officer ensures that all persons in his department, to whom the conditions of § 3 para. 1 points 1 to 2 apply, are security checked.

(4) The information security officer has to advise the responsible Federal Minister in matters of information security and to give suggestions for improvement if required.

Informationssicherheitskommission

§ 8. (1) Es wird eine Informationssicherheitskommission eingerichtet, der die Informationssicherheitsbeauftragten aller Bundesministerien angehören. Den Vorsitz führt der Informationssicherheitsbeauftragte des Bundeskanzleramtes. Die Informationssicherheitskommission hat

1. auf eine bundesweite Einheitlichkeit von Schutzmaßnahmen und deren Koordination im Bereich der Bundesverwaltung, insbesondere bei der Leistung von Amtshilfe nach § 5, hinzuwirken,
2. einen Erfahrungsaustausch hinsichtlich der Einhaltung von Schutzmaßnahmen nach § 7 Abs. 2 im jeweiligen Ressortbereich durchzuführen und gegebenenfalls Vorschläge zur Verbesserung der Informationssicherheit zu erstatten,
3. der Bundesregierung bei Bedarf, jedoch mindestens alle drei Jahre, einen Bericht über den Stand der Informationssicherheit auf Grundlage von Beiträgen der einzelnen Informationssicherheitsbeauftragten zu erstatten,
4. Maßnahmen zum Schutz des Austausches klassifizierter Informationen zwischen Österreich und internationalen Organisationen, sonstigen zwischenstaatlichen Einrichtungen oder fremden Staaten zu setzen beziehungsweise vorzuschlagen, sofern sie zur Durchführung der mit diesen über den Schutz und die Sicherheit klassifizierter Informationen getroffenen Vereinbarungen erforderlich sind,
5. Sicherheitsunbedenklichkeitsbescheinigungen für Personen, Unternehmen, Einrichtungen und Anlagen auszustellen.

(2) Die Informationssicherheitskommission gibt sich durch einstimmigen Beschluss eine Geschäftsordnung, die jedenfalls Regelungen hinsichtlich der Einberufung und des Geschäftsgangs von Sitzungen, der Organisation der Arbeiten sowie hinsichtlich der Willensbildung enthält.

(3) Soweit es für die ordnungsgemäße Wahrnehmung ihrer Aufgaben erforderlich ist, kann die Informationssicherheitskommission ihren Sitzungen auch sonstige Experten beiziehen. Näheres bestimmt die Geschäftsordnung.

Gerichtlich strafbare Handlungen

§ 9. (1) Wer entgegen den Bestimmungen dieses Bundesgesetzes eine ihm ausschließlich auf Grund von § 3 Abs. 1 dieses Bundesgesetzes anvertraute oder zugänglich gewordene, als „VERTRAULICH“, „GEHEIM“ oder „STRENG GEHEIM“ klassifizierte Information offenbart oder verwertet, deren Offenbarung

Information Security Commission

§ 8. (1) An Information Security Commission will be constituted, to which the information security officers of all Federal Ministries belong. The information security officer of the Federal Chancellery is the chairman. The Information Security Commission has to

1. work towards a nationwide uniformity of protective measures and its coordination in the area of the federal administration, particularly when providing administrative assistance as per § 5,
2. carry out an exchange of experience with regard to the compliance with protective measures as per § 7 para. 2 in each department and if necessary give suggestions for improving information security,
3. submit a report to the Federal Government when required, however at least every three years, on the state of information security on the basis of contributions of the individual information security officers,
4. implementing or suggesting measures for the protection of the exchange of classified information between Austria and international organisations, other intergovernmental institutions or foreign states, provided that they are required for the execution of agreements reached with them for the protection and security of classified information,
5. issuing security clearance certificates for persons, companies, institutions and facilities.

(2) The Information Security Commission, by a unanimous decision, decides the rules of procedure, which include at least regulations with regard to the convening and conducting of meetings, the organisation of the work as well as with regard to the decision making.

(3) Insofar as it is required for the proper execution of its duties, the Information Security Commission can also invite other experts to its meetings. Details will be specified in the rules of procedure.

Legally Punishable Offences

§ 9. (1) Whoever reveals or utilises, contrary to the regulations of this federal act, information entrusted or made accessible to him solely under § 3 para. 1 of this federal act, which is classified as "CONFIDENTIAL", "SECRET" or "TOP SECRET", the revelation or utilisation of which may compromise public safety, the

oder Verwertung geeignet ist, die öffentliche Sicherheit, die umfassende Landesverteidigung oder die auswärtigen Beziehungen zu beeinträchtigen, ist, sofern die Tat nicht nach anderen Bundesgesetzen mit strengerer Strafe bedroht ist, vom Gericht mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

(2) Wer die Tat begeht, um sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen, ist mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

(3) Offenbart der Täter Informationen, die verfassungsgefährdende Tatsachen (§ 252 Abs. 3 StGB) betreffen, so ist er nur zu bestrafen, wenn er in der Absicht handelt, private Interessen zu verletzen oder der Republik Österreich einen Nachteil zuzufügen. Die irrtümliche Annahme verfassungsgefährdender Tatsachen befreit den Täter nicht von Strafe.

Verwaltungsübertretung

§ 10. (1) Sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung erfüllt, begeht eine Verwaltungsübertretung,

1. wer die Verschwiegenheitspflicht nach § 4 Z 1 verletzt oder
2. wer entgegen § 4 Z 2 Schutzstandards nicht einhält, wenn dadurch ein Unbefugter Kenntnis von klassifizierten Informationen erlangt.

(2) Verwaltungsübertretungen nach Abs. 1 sind von der Bezirksverwaltungsbehörde mit Geldstrafe bis 3 000 Euro zu bestrafen.

2. Abschnitt

Sicherheitsunbedenklichkeitsbescheinigungen für Unternehmen und Anlagen

Anwendungsbereich des 2. Abschnitts

§ 11. Die Bestimmungen der §§ 11 bis 13 regeln die Ausstellung von Sicherheitsunbedenklichkeitsbescheinigungen für Unternehmen, Einrichtungen und Anlagen, die auf Grund völkerrechtlicher Verpflichtungen in unmittelbar anwendbaren Staatsverträgen gemäß Art. 50 Abs. 1 B-VG und Übereinkommen gemäß § 14 zur sicheren Verwendung klassifizierter Informationen für die Teilnahme an industriellen Tätigkeiten und Forschungstätigkeiten sowie zur Erlangung von Aufträgen erforderlich sind.

comprehensive national defence or foreign relations, has to be punished by the court with a prison sentence of up to six months or with a fine of up to 360 daily rates (based on income), provided that the crime is not punishable according to other federal laws with a more severe penalty.

(2) Whoever commits the crime, in order to gain for himself or anyone else a pecuniary advantage or to cause a detriment to anyone should be punished with a prison sentence of up to a year or with a fine of up to 360 daily rates.

(3) If the offender discloses information which concern facts endangering the constitution (§ 252 para. 3 StGB), he is to be punished, only if he acts with the intention to hurt private interests or to cause a disadvantage to the Republic of Austria. The mistaken assumption of constitution endangering facts does not free the offender from punishment.

Regulatory Offence

§ 10. (1) Insofar as the crime does not come under the category of a punishable offence falling within the jurisdiction of the courts, a person commits a regulatory offence,

1. if he violates the obligation of secrecy as per § 4 point 1 or
2. if he does not comply with the protection standards as per § 4 point 2, if through this an unauthorised person gets access to classified information.

(2) Regulatory offences as per para. 1 have to be punished by the district administration with a fine of up to 3000 euros.

2nd Section

Security Clearance Certificates for Companies and Facilities

Scope of the 2nd Section

§ 11. The regulations of §§ 11 to 13 regulate the issue of security clearance certificates for companies, institutions and facilities, which are required, due to obligations under international law in immediately applicable international treaties as per Art. 50 para. 1 [Federal Constitutional Law](#) and agreements as per § 14, for secure use of classified information for participation in industrial activities and research activities as well as for getting orders.

Ausstellung und Widerruf von Sicherheitsunbedenklichkeitsbescheinigungen

§ 12. (1) Der Antrag auf Ausstellung von Sicherheitsunbedenklichkeitsbescheinigungen ist bei dem für die betreffende industrielle Tätigkeit oder Forschungstätigkeit oder für die Art des vorgesehenen Auftrages nach dem Bundesministerengesetz 1986, BGBl. Nr. 76, sachlich zuständigen Bundesminister zu stellen.

(2) Vor Entscheidung über die Ausstellung einer Sicherheitsunbedenklichkeitsbescheinigung ist der Bundesminister für Inneres zu hören. Diesem obliegt die Mitwirkung an der Feststellung, ob eine Einrichtung den in der Informationssicherheitsverordnung (§ 6) vorgesehenen Schutz für klassifizierte Informationen der im Antrag bezeichneten Klassifizierungsstufe gewährleisten kann.

(3) Bei der Mitwirkung an der Entscheidung nach Abs. 2 sind auch alle Personen, die zur Erfüllung ihrer beruflichen Pflichten Zugang zu Informationen haben müssen, die als „VERTRAULICH“, „GEHEIM“ oder „STRENG GEHEIM“ klassifiziert wurden, einer Sicherheitsüberprüfung gemäß §§ 55 bis 55b des Sicherheitspolizeigesetzes, BGBl. Nr. 566/1991, zu unterziehen. Das Ergebnis ist dem zuständigen Bundesminister (Abs. 1) mitzuteilen.

(4) Die Voraussetzungen für die Ausstellung einer Sicherheitsunbedenklichkeitsbescheinigung sind gegeben, wenn die in der jeweiligen völkerrechtlichen Verpflichtung vorgesehenen Auflagen und Bedingungen vom Antragsteller erfüllt werden. Der zuständige Bundesminister hat durch Sicherheitsinspektionen die Einhaltung dieser Auflagen und Bedingungen regelmäßig zu überprüfen. Dabei ist der Bundesminister für Inneres zu hören. Die Sicherheitsunbedenklichkeitsbescheinigung ist zu widerrufen, wenn

1. die Voraussetzungen ihrer Ausstellung weggefallen sind oder
2. das Unternehmen oder Einrichtung den Sicherheitsinspektionsorganen den Zutritt in dem für die Überprüfung notwendigen Ausmaß innerhalb der üblichen Geschäfts- oder Arbeitszeit zu ihren Grundstücken, Geschäfts- und Betriebsräumen zu Unrecht verweigert oder die erforderliche Mitwirkung bei der Überprüfung unterlässt.

(4a) Die Ausstellung und der Widerruf der Sicherheitsunbedenklichkeitsbescheinigung erfolgen auf Vorschlag des zuständigen Bundesministers (Abs. 1) durch die im jeweiligen völkerrechtlichen Übereinkommen vorgesehene nationale Zertifizierungsstelle. Diese ist, sofern nicht ausdrücklich eine andere vorgesehen ist, die Informationssicherheitskommission

Issue and Revocation of Security Clearance Certificates

§ 12. (1) The application for issuing security clearance certificates has to be submitted to the Federal Minister who is responsible for the respective industrial activity or research activity or for the particular contract according to the Federal Ministries Law 1986, FLG no. 76.

(2) Before deciding on the issue of a security clearance certificate the Federal Minister for Home Affairs must be consulted. They take the decision together, whether an institution can ensure the protection for classified information of the classification level described in the application as per the Information Security Ordinance (§ 6).

(3) While working on the decision as per para. 2, all persons who require access to information, which was classified as "CONFIDENTIAL", "SECRET" or "TOP SECRET", for the fulfilment of their professional duties should also undergo a security check as per §§ 55 to 55b of the Security Police Act, FLG no. 566/1991. The result should be communicated to the concerned Federal Minister (para. 1).

(4) The prerequisites for issuing a security clearance certificate exist, if the applicant satisfies the constraints and conditions required by the respective obligation under international law. The concerned Federal Minister has to regularly verify the compliance with these constraints and conditions by security inspections. In this the Federal Minister for Home Affairs should be consulted. The security clearance certificate has to be revoked, if

1. the prerequisites for issuing it do not exist anymore or
2. the company or institution wrongly refuses the security inspection officials access during the usual business or working hours to their properties, business and operating rooms to the extent necessary for the inspection or does not provide the required cooperation during the inspection.

(4a) The issue and revocation of the security clearance certificate are carried out, on recommendation of the responsible Federal Minister (para. 1), by the national certification authority specified by the respective agreement under international law. This is the Information Security Commission at the Federal Chancellery (§ 8), provided nothing else is expressly mentioned. For the issue of the

beim Bundeskanzleramt (§ 8). Für die Ausstellung von Sicherheitsunbedenklichkeitsbescheinigungen im Zusammenhang mit Vorhaben, die der Erfüllung von Aufgaben des Bundesheeres gemäß Art. 79 Abs. 1 B-VG dienen, ist die nationale Zertifizierungsstelle eine vom Bundesminister für Landesverteidigung für zuständig erklärte Dienststelle seines Wirkungsbereiches. Die Sicherheitsunbedenklichkeitsbescheinigung ist von der Zertifizierungsstelle der Einrichtung zu übermitteln, zu deren klassifizierten Informationen der Antragsteller Zugang haben möchte; dies gilt auch für den Widerruf. Der Antragsteller ist über die Ausstellung oder den Widerruf zu verständigen.

(4b) Wenn Personen im Ausland Zugang zu klassifizierten Informationen oder Zutritt zu Örtlichkeiten einer erhöhten Sicherheitsstufe erhalten sollen, dürfen im Rahmen des internationalen Besuchskontrollverfahrens die sie betreffenden personenbezogenen Daten mit ihrer Einwilligung der Einrichtung, die für die Sicherheit des Zugangs zu den betreffenden Informationen oder Örtlichkeiten zuständig ist, übermittelt werden. § 25 MBG bleibt unberührt.

(5) Kann eine Sicherheitsunbedenklichkeitsbescheinigung nicht ausgestellt werden, hat der zuständige Bundesminister (Abs. 1) den Antragsteller hiervon unverzüglich nach Kenntnis dieses Umstandes schriftlich zu informieren.

(6) Ist der Antrag im Sinne des Abs. 1 beim Bundesminister für Landesverteidigung zu stellen, so obliegt diesem die Feststellung, ob eine Einrichtung den in der Informationssicherheitsverordnung (§ 6) vorgesehenen Schutz für klassifizierte Informationen der im Antrag bezeichneten Klassifizierungsstufe gewährleisten kann. Abs. 3 ist mit der Maßgabe anzuwenden, dass an Stelle der Sicherheitsüberprüfung eine Verlässlichkeitsprüfung gemäß §§ 23 und 24 Militärbefugnisgesetz, BGBl. I Nr. 86/2000, durchzuführen ist. Der Bundesminister für Landesverteidigung ist ermächtigt, durch Verordnung eine dem Bundesministerium für Landesverteidigung nachgeordnete Dienststelle an seiner Stelle mit der Wahrnehmung dieser Aufgaben zu betrauen.

Kostenersatzpflicht

§ 13. Für die Ausstellung einer Sicherheitsunbedenklichkeitsbescheinigung gebührt dem Bund als Ersatz ein Pauschalbetrag, der durch Verordnung des sachlich zuständigen Bundesministers im Einvernehmen mit dem Bundesminister für Inneres entsprechend den tatsächlichen durchschnittlichen Kosten festgelegt wird. In den Fällen des § 12 Abs. 6 ist dieses Einvernehmen nicht erforderlich. Weiters hat der Antragsteller dem Bund die Barauslagen für Sachverständige zu ersetzen,

security clearance certificates in connection with activities, which serve the fulfilment of tasks of the armed services as per Art. 79 para. 1 [Federal Constitutional Law](#), the national certification authority is an office within that department, declared by the Federal Minister for National Defence to be responsible for this activity. The security clearance certificate is to be sent by the certification authority to the institution, the classified information of which the applicant wants to have access to; this also applies to the revocation. The applicant has to be informed about the issue or the revocation.

(4b) When persons abroad are to be given access to classified information or access to places having an increased security level, in the framework of the international visit control procedure, the personal data concerning them may be transmitted with their consent to the institution, which is responsible for the security of the access to the information or places in question. § 25 MBG remains untouched.

(5) If a security clearance certificate cannot be issued, the responsible Federal Minister (para. 1) has to inform the applicant of it in writing immediately after receiving knowledge of this circumstance.

(6) If the application has to be made to the Federal Minister for National Defence as per para. 1, then the latter has to confirm, whether an institution can ensure the classification level described in the application for the protection of classified information provided by the Information Security Ordinance (§ 6). Para. 3 has to be applied with the stipulation, that in lieu of the security check a reliability test has to be carried out as per §§ 23 and 24 Armed Forces Authority Act, FLG 1 no. 86/2000. The Federal Minister for National Defence is authorised to entrust by ordinance a subordinate office of the Federal Ministry of national defence with the execution of these tasks in his place.

Obligation to pay Compensation

§ 13. For the issue of a security clearance certificate a flat sum is due to the Federal Government as compensation, which is determined by an ordinance of the responsible Federal Minister in agreement with the Federal Minister for Home Affairs based on the actual average costs. This agreement is not required in the cases of § 12 para. 6. The applicant has to reimburse the out-of-pocket expenses of experts to the Federal Government, even if the application for the issue of a security clearance certificate is not successful.

auch wenn dem Antrag auf Ausstellung einer Sicherheitsunbedenklichkeitsbescheinigung nicht gefolgt wird.

3. Abschnitt Gemeinsame Bestimmungen

Internationale Übereinkommen

§ 14. (1) Sofern die Bundesregierung oder die zuständigen Mitglieder der Bundesregierung zum Abschluss von Übereinkommen gemäß Art. 66 Abs. 2 B-VG ermächtigt sind, können sie völkerrechtliche Vereinbarungen schließen, um den gegenseitigen Austausch und den Schutz klassifizierter Informationen zu regeln. Hierbei ist vorzusehen, dass klassifizierte Informationen nur dann übermittelt werden dürfen, wenn beim Empfänger ein Schutzstandard gewährleistet ist, der dem der übermittelnden Stelle gleichwertig ist.

(2) Übereinkommen gemäß Abs. 1 können insbesondere Folgendes regeln:

1. den Zugang von Personen der jeweils anderen Vertragspartei zu klassifizierten Informationen,
2. die Ausstellung von Sicherheitsunbedenklichkeitsbescheinigungen,
3. die Auflagen und Bedingungen für die Ausstellung von Sicherheitsunbedenklichkeitsbescheinigungen,
4. die Voraussetzungen für den Widerruf von Sicherheitsunbedenklichkeitsbescheinigungen,
5. die Zustellung von klassifizierten Informationen für Unternehmen an die zuständige Behörde der jeweils anderen Vertragspartei und die Verpflichtung der zuständigen Behörde, diese Informationen nach deren Klassifizierung entsprechend den Geheimhaltungsstufen des Übereinkommens den Unternehmen weiterzuleiten,
6. den Einsatz von bestimmten Zustelldiensten und Verschlüsselungsgeräten,
7. die Zustellung der Sicherheitsunbedenklichkeitsbescheinigungen und deren Widerruf an die zuständige Behörde der jeweils anderen Vertragspartei.

Sprachliche Gleichbehandlung

§ 15. Die in diesem Bundesgesetz verwendeten personenbezogenen Ausdrücke betreffen, soweit es inhaltlich in Betracht kommt, Frauen und Männer gleichermaßen.

3rd Section Common Regulations

International Agreements

§ 14. (1) Provided that the Federal Government or the responsible members of the Federal Government are authorised as per Art. 66 para. 2 [Federal Constitutional Law](#) to conclude agreements, they can conclude agreements under international law to regulate the mutual exchange and the protection of classified information. Here it has to be ensured that classified information may only then be transmitted if the receiver ensures a protection standard equal to that of the transmitter.

(2) agreements as per para. 1 can particularly regulate the following:

1. the access of persons of the other contracting party to classified information,
2. the issue of security clearance certificates,
3. the constraints and conditions for the issue of security clearance certificates,
4. the prerequisites for the revocation of security clearance certificates,
5. the delivery of classified information for companies to the responsible authority of the other contracting party and the obligation of the responsible authority, to forward this information after classification according to the levels of secrecy of the agreement to the companies,
6. the introduction of certain delivery services and encryption equipment,
7. the delivery of the security clearance certificates and their revocation to the responsible authority of the other contracting party."

Equal Treatment in Language

§ 15. The expressions referring to persons used in this federal act, as far as the content is concerned, refer to women and men equally.

Verweisungen

§ 16. Verweisungen in diesem Bundesgesetz auf andere Bundesgesetze verweisen auf deren jeweils geltende Fassung.

Vollziehung

§ 17. Mit der Vollziehung dieses Bundesgesetzes ist die Bundesregierung, jedoch in Angelegenheiten, die nur den Wirkungsbereich eines Mitglieds der Bundesregierung betreffen, dieses betraut.

Inkrafttreten

§ 18. (1) § 3 Abs. 1 und § 12 Abs. 4b in der Fassung des Materien-Datenschutz-Anpassungsgesetzes 2018, BGBl. I Nr. 32/2018, treten mit 25. Mai 2018 in Kraft; gleichzeitig tritt § 3 Abs. 3 außer Kraft.

(2) § 2 Abs. 1 und 2 in der Fassung des Informationsfreiheits-Anpassungsgesetzes, BGBl. I Nr. 50/2025, tritt mit 1. September 2025 in Kraft.

Cross References

§ 16. Cross references in this federal act to other federal acts refer to the respectively current versions.

Execution

§ 17. the Federal Government is entrusted with the execution of this federal act. However, in matters which concern only the sphere of action of a member of the Federal Government, he is responsible for the execution.

Legal Validity

§ 18. § 3 (1) and § 12 (4b) in the version of the Data Protection Adaption Act 2018, Federal Law Gazette I No. 32/2018, enter into force on 25 May 2018; at the same time § 3 (3) expires.