Bundesministerium
Inneres

Direktion Staatsschutz
und Nachrichtendienst

Information sheet on the security vetting pursuant to sections 55 et seqq. of the Security Police Act (SPG)

Pursuant to § 55 (1) SPG, security vetting is the process **of checking an individual's reliability** on the basis of personal data that provide information on whether there is any reason to believe that the individual will carry out dangerous attacks. In the framework of the security vetting personal data is used that have been investigated by the security authorities in the enforcement of federal or state laws; furthermore, data may be requested from other authorities or otherwise investigated if the data subject occupies or seeks to occupy a position that involves access to secret information.

Pursuant to § 55 (3) SPG, information is classified as

1. 1. **"confidential"** if it is subject to secrecy protection pursuant to criminal law and its non-disclosure is in the public interest;
2. 2. **"secret"** if it is confidential and its disclosure would entail the risk to cause substantial damage to the economic interests of a federal, regional or local authority, to public safety or to national comprehensive defence;
3. 3. **"top secret"** if it is secret and its disclosure would additionally be likely to cause severe damage pursuant to § 55 (3) item 2 SPG.

Security vetting may be carried out (according to § 55a (1) SPG):

1. in order to ensure the lawful exercise of duties or the non-disclosure of confidential information;
2. in order to provide preventive protection to officials of constitutional institutions (§ 22 (1) item 2 SPG) and to representatives of foreign states, international organisations or other subjects of international law (§ 22 (1) item 3 SPG) with regard to individuals who are in the physical surroundings of the protected person.

Security vetting to ensure the lawful exercise of duties or the non-disclosure of confidential information shall be carried out (in accordance with § 55a (2) SPG):

1. upon request of the authority in which the data subject occupies or seeks to occupy a position as a regular staff member, which involves issuing direct orders or executing coercive measures in administrative matters or significantly influencing the realisation of other administrative acts or other important administrative decisions;

Last updated: 02/2025

2. upon request of the Federal Minister of Foreign Affairs prior to granting an exequatur to the head of a consular representation or an agrément to the head of a diplomatic mission;

3. upon well-founded request of the company in which the data subject occupies or seeks to occupy a position involving access to confidential information, which, if used in a foreign country (§ 124 of the Austrian Penal Code (StGB)), may cause damage to the company;

3a. upon well-founded request of the company in which the data subject occupies or seeks to occupy a position involving access to confidential information, which, if used improperly, may cause lasting malfunction or destruction to a critical infrastructure (§ 22 (1) item 6 SPG);

4. if the data subject is to receive access to information obtained through surveillance measures as defined in § 136 (1) item 3 of the Austrian Code of Criminal Procedure (StPO);

5. if the data subject is 18 or over and lives in the same household as a person who has access to top secret information.

Furthermore, a security vetting shall be carried out upon the request of an institution of the European Communities or other international organisation if an Austrian citizen or a person with main residence in Austria is to occupy a position that requires access to confidential information of this organisation.

Except in cases of preventive protection of officials and prior to the granting of an exequatur or agrément, a security vetting may only be carried out with the consent and on the basis of a declaration of the data subject regarding his/her past and current personal circumstances (security declaration). Furthermore, the data subject must consent to the transmission of the result of the security vetting to the employer or the requesting authority.

Security vetting based on security declarations is performed centrally by the Directorate State Protection and Intelligence Service (BMI-II/DSN/S4). The Directorate State Protection and Intelligence Service processes the data within the framework of its file management. In this regard, we refer to § 43 of the Federal Act concerning the Protection of Personal Data (DSG) according to which the data subject must be informed on the processing of the data within the EDIS file management system (office automation).

Security vetting at the request of companies is subject to a fee of €297.00, €593.00 or €890.00, depending on the confidentiality level. The fees shall be paid by the requesting company. The security vetting is carried out after the payment has been made.

Information on how to complete the applications correctly:

- Make sure that you answer all questions on the security declaration form.
- You must add the current date to the signature.
- The signature must be either handwritten or made via digital signature.
- The security declaration must contain a copy of the identification document mentioned therein (passport or identity card).
- Make sure that you submit each security declaration (also those of co-residents) individually so that each security declaration only contains the data of the respective individual to be vetted.

<u>Applications that are not filled in correctly will be returned without being processed.</u>

Security declarations

- Security declarations classified as **“confidential”** must be made using **annex A**.
- Security declarations classified as **“secret”** must be made using **annex B**.
- Security declarations classified as **“top secret”** must be made using **annex C** and
- Security declarations by persons aged 18 or over who live in the same household as an individual who has access to top secret information **(co-residents)** must be made using **annex D**.