Foreword

Annually the General Intelligence and Security Service (AIVD) and the Military Intelligence and Security Service (MIVD) conduct tens of thousands security screenings of persons who (are about to) take up positions involving confidentiality. These positions are posts in which an abuse of office could endanger national security. A person cannot take up a position involving confidentiality until the AIVD or the MIVD has granted them Security Clearance. Conducting security screenings enables the AIVD and the MIVD to – in time – discern vulnerabilities that could pose a risk to national security.

Lately, the demand for transparency about the criteria the services use during a security screening has grown. This guide will provide an insight into the personal conduct and circumstances, which will be part of the security screening process of the applicant for a position involving confidentiality. We believe that this explanation of the criteria, indicators and possibilities for objections and appeals will provide employers and (future) officials in positions involving confidentiality further clarity about the security screening process.

Dr G. ter Horst
Minister of the Interior and Kingdom Relations

E. van Middelkoop
Minister of Defence

Contents

Personal conduct and circumstances guide

A clarification of how personal conduct and circumstances are relevant to security screenings by the AIVD and MIVD.

The Cause

Recently, questions have risen in public debate about the manner in which the General Intelligence and Security Service (AIVD) and the Military intelligence and Security Service (MIVD) conduct security screenings. Often these questions were prompted by specific cases in publicity. Since a security screening can have far-reaching consequences for the privacy and sense of social security of the person under scrutiny, the services cannot publicly reveal individual matters. Nevertheless, in order to provide more insight into the framework that the services use in their investigations, this guide will expound on personal conduct and circumstances within the security screening process.

The Security Screening process

Persons who will take up a position involving confidentiality have to undergo security screening. Because an abuse of office could seriously endanger national security or other important state interests, positions involving confidentiality are determined by the ministers in the relevant government department. The aim of this security screening is to minimise any risks by investigating whether a person is vulnerable. During this screening process various aspects in the life of the person in question are investigated. Therefore, a person who aspires to a function that is designated a position involving confidentiality may expect questions and requests for information about their circumstances at work and their private life. During such a drastic screening process their privacy will always be protected as much as possible.

Goal

This guideline strives to clarify how personal conduct and circumstances are relevant to security screenings. To this purpose the framework that is used by the services during their investigations will be described. If a service grants Security Clearance, which takes the form of a “verklaring van geen bezwaar” (VGB), (literally “a statement of no objection”), it has no objection on national security grounds to the subject taking up the position involving confidentiality. The security screening process always leads to a decision specifically meant for a certain person in a certain position. First this guideline will explain on which principles an assessment is based. Subsequently, it will deal with the criteria a person filling a post involving confidentiality has to meet and which indicators may point to any risks and vulnerabilities. And finally it will clarify how the screening is regulated and how the procedure of appeals is organised.

1. Basic principles of assessment

Custom made

A number of indicators are mentioned in this guide, which may be of importance during a security screening. In general, these matters may play a role in all security screenings. Assessing these indicators, however, always differs from case to case. The reason for this is that every position has its specific vulnerabilities. Therefore, the specific demands of every position involving confidentiality are taken into account during the assessment. Positions involving confidentiality that are so designated because of the integrity that is needed, demand a different level of integrity from a candidate than functions that are so designated because of constant exposure to state secrets. Where positions designated on basis of integrity are concerned, national security and other important state interests are at stake because a lapse of integrity would – above all – seriously harm the prestige of the Dutch government. In addition, the context within which conduct or circumstances arise will always be considered too. All these factors make every security screening a custom-made one. This individual assessment is clearly stipulated by the Security Screening Act.

Recognizable, factual conduct

In order to be able to recognize a person's vulnerabilities, their personal conduct and circumstances are investigated during the screening, that is to say; their recognizable, factual conduct and factual circumstances. If – during the screening – information comes to light about conduct or circumstances that might make the party involved vulnerable, there has to be a sufficient amount of data to make it plausible that this conduct has taken place or is taking place. Thus, it is avoided that an assessment of vulnerability is based on hearsay or insinuations and cannot be sufficiently substantiated.

Vulnerability as a risk

During a security screening the service forms an opinion about the vulnerability of a certain person in relation to a particular position involving confidentiality. Such vulnerability – if it exists – poses a risk to national security or other important interests of the state. Security Clearance (VGB) will not be refused or withdrawn solely based on a certain type of conduct or circumstance. The assessment is always based on the vulnerability which may result from personal conduct and circumstances. Therefore, moral judgment about personal conduct or circumstances is not relevant at all within the framework of a security screening process. The investigation limits itself to potential vulnerabilities of a specific person in a specific confidential position. Therefore, the screening process focuses on the person in question. Their environment and specifically the partner, if there is one, are also screened to establish whether the person in question has any vulnerabilities.

2. Criteria

Honesty
To be able to take up a position involving confidentiality reliably, it is important that the person in question provides relevant facts and information in an honest way. If it can be established that the person in question consciously gives incorrect facts or consciously withholds relevant information, regardless whether they intend to mislead or not, their conduct is deemed dishonest.

Independence
The person in question must be able to perform the position involving confidentiality independently. Dependence may be the result of personal conduct, such as an addiction or serious financial problems. This could impair a person's judgement. Personal environment could also generate dependence, for example a person in question may be (undesirably) influenced by their partner, family, friends or foreign governments.

Loyalty
A security screening must also establish whether the person in question feels sufficient loyalty towards the employer, Dutch society and democratic legal order. A person in a position involving confidentiality, who has problems with loyalty, may harm national security if they have a lapse of integrity. Problems with loyalty towards Dutch society and democratic legal order can also pose danger for national security and other important state interests.

Integrity
Integrity is a quality which corresponds to the principles justice, honesty and equality. Integrity means that one performs one's tasks and handles one's authority conscientiously. Integrity in a government position involving confidentiality is a fundamental principle for national security because otherwise why would citizens need to accept government authority and adhere to laws and regulations. Every citizen has to be able to trust in the integrity of a government official who takes up a confidential position.

Based on these criteria an assessment is made whether the person in question has the intention to fulfil the position involving confidentiality reliably and if he or she could be deemed capable to do so.

3. Indicators

Criminal Records

If a person has a criminal record it could mean that there might not be enough guarantees that they would conduct themselves reliably in their position involving confidentiality. A criminal record can suggest that someone has a problem with honesty, independence, loyalty or integrity. To establish whether conduct that leads to a criminal record makes a person vulnerable in their confidential position, certain factors are taken into account: did it happen recently or not, what was the nature and severity of the offence, how severe was the punishment that was imposed and how many offences were recorded. Furthermore, the age of the person in question at the time of the offence is also considered. The evaluation process of any criminal records of (candidate) officials in positions involving confidentiality is strictly regulated by policies, which have been especially developed for various sectors.

Subversive and anti-democratic activities

An important indicator is whether someone takes part in or supports activities that may harm national security. So is membership of or support to organisations with goals that strongly suggest that they could endanger lasting democratic legal order. Subversive and anti-democratic activities may also manifest themselves through the means that are used to obtain certain goals[1]. In this context it is important to investigate certain areas of attention, such as terrorism, violent activism, extremism, espionage, proliferation of mass destruction weapons and organised crime.

Addictions

An addiction leads to physical and/or psychological dependence. Such dependence may manifest itself through excessive use of alcohol, drugs or other substances that influence one's behaviour. One can also be addicted to gambling or sex. Behaviour that emanates from such an addiction may cause a person to become incapable of fulfilling a position involving confidentiality reliably. Moreover, if forbidden substances, such as drugs, are involved there is also the risk of a criminal connection.

Financial vulnerability

Financial vulnerability can be caused by severe financial problems. Such vulnerability may be determined by considering a person's attitude towards the size of the debt, their capital and their income and expenditure pattern.
Someone's financial situation may cause a person to be considered vulnerable to bribery or blackmail. There is also a risk that when someone has severe financial problems, they might not be able to resist temptations such as handling stolen goods or selling confidential information.

Undesired Influence

The nature of a relationship with certain persons, organisations or foreign governments may suggest potential undesired influence, which could cause a person to be impaired in their fair and independent judgement. For example, an acquaintance with a criminal background could incite the person in question to undesirable behaviour. Contact with a foreign intelligence service constitutes a significant vulnerability, which the person in question is often not even aware of. Because of the risk involved, this fact may lead to a refusal or withdrawal of a VGB. Membership of a faction that limits a person's autonomy considerably (often referred to as a *sect*) can also be an indicator of undesired influence. The strong pressure of loyalty to the family or the

[1] See article 7, paragraph 2, b and c of the Security Screening Act, 10 October 1996.

country of origin can also pose a risk and lead to undesired influence.

Deceitful or Secretive behaviour

Deceitful behaviour means that someone knowingly makes incorrect statements and/or deliberately paints an incomplete picture. Deceitful behaviour also means distorting facts and/or withholding required or relevant information with the intention to mislead. Secretive behaviour means to have a secret that could have negative consequences for the person in question or their surroundings were it to be revealed. Therefore, deceitful or secretive behaviour can make a person vulnerable to blackmail by others and could cause them to exhibit lack of integrity.

Lapse of integrity

A lapse of integrity in one's behaviour means that – for example – the regard and authority of the function a person fills is compromised and thus the employer and national security and/or other important state interests are damaged. A lapse of integrity may occur in the working place but also outside of it. A lapse of professional integrity means that one uses the authorities that are begotten in one's function improperly.

Irresponsible and risky behaviour

Irresponsible and risky behaviour can mean that a person does not heed the physical integrity and safety of others. Also it can manifest itself in risky, irresponsible expenditure or other forms of impulsive behaviour that can ultimately pose a risk to national security.

These are the indicators that may point out that someone is vulnerable or poses a risk to national security.

4. Supervision and Objection procedure

Due diligence and supervision

During the security screening process the services gather information provided by the person in question, data bases and by persons who are acquainted with the person under investigation. They do not use special powers, such as eavesdropping on telecommunications. The law does not allow this.

To guarantee a conscientious and diligent procedure the services have regulated the manner in which a security screening is conducted. The various functions within the research team have been separated to guarantee an objective assessment of the gathered information. The overall assessment for example, is not done by the employee who performed the interviews, but by a different person. In addition, diligence is secured by constant mutual supervision of colleagues. The (independent) Intelligence and Security Services Regulatory Committee (CTIVD) supervises – among other things – the lawful execution of the Security Screening Act. For this purpose, the committee has full access to all relevant information and may, if it so wishes, contact all persons involved, also employees of the services.

Objections and appeals

When a service concludes that, based on the security screening, there are not enough guarantees that a person will fill the position involving confidentiality faithfully under all circumstances, it issues an intention to refuse (or withdraw) the VGB. This gives the person in question a chance to voice their opinion, after which the service may re-evaluate its decision. Although, in certain cases the service decides to immediately withdraw or refuse a VGB. One can lodge a complaint against refusal or withdrawal of a VGB with a committee of appeal. This committee hears the person involved and also the service and views the file. On that basis it issues an advice to the Minister of the Interior and Kingdom Relations or the Minister of Defence concerning the appeal. Thereafter the decision is either confirmed or revised by the Minister. If the person in question does not agree with this decision they can lodge an appeal with the court and a further appeal with the Council of State.

A person is only allowed to inspect their security screening file with certain restrictions. The sources which have been interviewed during the investigation remain secret. Because the legal rights of the person in question have to be safeguarded, the court and the Council of State are allowed complete access to the file, also the secret part of it. The person in question, however, must give the court or the Council of State permission to do that.