Instruction booklet

Guidelines on the safeguarding of CI by businesses

1. General information

All members of staff at your company who have authorised access to state secrets (classified information) or work in a security-sensitive area carry particular responsibility for ensuring the security of their fellow employees, the company, and the Federal Republic of Germany. The following guidelines are intended to provide such staff with basic information on the most important measures that need to be taken in order to protect classified government information. They also deal with potential threats (terrorism, extremism, criminal activity such as (industrial) espionage by rival companies or foreign intelligence services).

The rules on protecting classified information (CI) must be followed carefully. Any limitations, inconveniences, or delays that are caused as a result of doing so must be tolerated in order to ensure that the CI, and your company and its staff, are adequately protected.

The political changes that have taken place around the globe continue to be one reason why the Federal Republic of Germany and its companies are a particular target for (industrial) espionage by foreign intelligence services seeking to gain classified information/state secrets. Those who commit treason not only harm our country, their employer, and their colleagues, but also themselves. They often only realise the way in which they have been taken advantage of much later on.

Anyone can become a target for competitors, terrorist organisations, or foreign intelligence services, without it being their fault.

The only way to escape the snare of intelligence services or get out of a situation whereby you have been betraying information in another way (e.g. reckless disclosure of CI to competitors/reckless disclosure of information on the way security measures work with terrorist organisations etc.), without incurring personal damage, is to voluntarily approach the relevant authority and explain what has been going on. In a large number of cases, the constitution protection authorities will be able to refrain from pressing charges. Criminal law also provides that immunity from prosecution can be provided in such cases (Section 153 e of the Code of Criminal Procedure). Make use of this opportunity – both in your own interest and in the interest of our liberal state based on the rule of law.

Your key point of contact in all issues of security is the information security officer appointed by your company management. You can approach him or her in all security-related matters. The information security officer must treat all personal matters linked to the protection of classified information confidentially.

2. Why do we have classified information?

In a liberal democracy, the actions of the state are based on the principle of transparency, meaning that, in principle, they are transparent for all. In the interests of external and internal security and the protection of businesses and citizens, the democratic state must, however, also keep specific information secret.

The Federal Republic of Germany is part of an international coalition that is fighting terrorism, and is therefore a potential target for attacks. The reckless disclosure of information on the way in which security measures are organised and operate in your company could make such attacks possible or more simple to carry out. In addition, if CI regarding the building of war weapons, for example, gets into the wrong hands, there is considerable potential for this to put our global ability to counter terrorist attacks at risk.

Competitors are interested in obtaining the relevant expert knowledge held by your company without having to invest in expensive and lengthy research processes etc. As a member of staff at your company, you carry particular responsibility for protecting this information, particularly when it is classified.

Most countries conduct reconnaissance abroad through their security services. The countries on which this intelligence is gained consider this as espionage, which is liable to heavy sanctions due to the potential political, military, and economic damage that this can cause. Due to its economic and political importance as well as its geographical location, the Federal Republic of Germany is a major espionage target for foreign intelligence services.

In order to protect classified information, persons intended to access it undergo security clearance to ensure their suitability to access it. Security clearance is undertaken in accordance with the Security Clearance Check Act (Section 25 of the Law on Prerequisites and Procedures for Security Clearance Checks Undertaken by the Federal Government of 20 April 1994 –Federal Law Gazette I page 867), which takes account of minimum requirements by which the Federal Republic of Germany is contractually bound not least vis-à-vis foreign countries and as a member of

intergovernmental organisations (such as NATO, OCCAR), or legally bound as part of the EU.

At the same time, the provisions on the protection of personal data set out in the Federal Data Protection Act must also be followed (see Section 36 subsection 1 and 2 of the Security Clearance Check Act).

3. The safeguarding of classified information – main points in brief

3.1. The term classified information (CI)

The term classified information is used to describe facts, objects, or knowledge that needs to be treated as confidential – irrespective of the form of the CI (e.g. written material, drawings, cards, photocopies, photographs, magnetic memory, electrical signals, devices, or technical equipment, as well as the spoken word). They are classified by public bodies/on the instructions of public bodies as either TOP-SECRET, SECRET, CONFIDENTIAL, or CONFIDENTIAL MATERIAL – FOR OFFICIAL USE ONLY.

3.2. The classification of information

The classification of information is undertaken by a public body (authority) and will be communicated to you by this body in the form of a list of classified items or other written document (e.g. when there is only a small number of classified items). The CI is to be treated in strict accordance with its classification at all times (– this includes future contracts taken on by your company in which information that has been previously classified is to be used). If the handling of a particular piece of information in accordance with its classification proves to be impracticable, you must inform your information security officer immediately, who will clarify the issue with the public body from which the CI originates, and with the Federal Ministry for Economic Affairs and Climate Action.

3.3. CI is based on the ‘need-to-know’ principle

Information that has been classified as CONFIDENTIAL or higher may only be accessed by persons who have undergone security clearance and who are authorised to do so.

Such persons are only to access CI in as far as this is absolutely necessary in order for them to carry out their work. This rule also applies to the closest colleagues of persons accessing the CI, from whom this information must also be kept secret. Persons of trust (spouses, partners, companions, friends, doctors etc.) must never be informed about the content of CI.

In most cases of espionage and betrayal of information, the level of damage caused could have been limited if the 'need-to-know' principle had been observed.

3.4. Confidentiality

Do not discuss CI or other important information in the presence of persons unauthorised to access it, or in public (pubs, trains, aeroplanes, etc.). When discussing or processing CI, use meeting rooms (which may be bug-proof or tap-proof) and control/exclusion zones that your information security officer has specially assigned for this purpose. Follow all of the instructions for working in these areas closely (e.g. access checks, camera and mobile phone ban, wearing of company ID to be visible at all times, etc.).

3.5. Personal responsibility, passing on of CI

CI that has been classified as CONFIDENTIAL or higher may only be passed on to persons authorised to access it via the CI registry and only once a confirmation of receipt has been signed. A list of persons at your company who are authorised to consult CI is held by the information security officer and the CI administrator. You are personally responsible for protecting any CI that you have received from the CI registry. You must return the CI to the registry as soon as possible. It is prohibited for CI to be passed on to another colleague at the company directly. This must go via the CI registry, which frees you of your responsibility for protecting it and passes this responsibility on to your colleague.

Do not leave CI unattended at your work station, even for a short amount of time; make sure that no unauthorised persons are able to consult it. Your information security officer will provide you with more detailed information on this.

You are also personally responsible for any CI that may be mistakenly passed on to you in another way, without going through the CI registry first. If this happens, you must inform your CI registry and information security officer immediately.

The rules that apply to CI classified as CONFIDENTIAL MATERIAL – FOR OFFICIAL USE ONLY are less stringent. Anyone who has received CI classified at this level must have signed that they have read the information sheet on this level of CI, comply with the rules, and maintain confidentiality. The 'need-to-know' principle must also be observed. Ask your information security officer for more details.

3.6. Production and duplication of CI, classified waste (classified as CONFIDENTIAL or higher)

CI that has been classified as CONFIDENTIAL or higher many only be generated in areas cleared for this purpose (individual rooms, control or exclusion zones, etc.)

Intermediate or by-products generated in the process of producing or duplicating CI and which themselves contain CI in some kind of form (e.g. handwritten drafts, computer discs) are to be protected in the same way as CI and to be reported to the registry, which will decide how they are to be dealt with.

3.7. Storage, sending, and borrowing of CI

CI that has been classified as CONFIDENTIAL or higher is to be stored in the CI registry. CI that has been classified as CONFIDENTIAL MATERIAL – FOR OFFICIAL USE ONLY can be stored in a locked room (individual lock; not master key system) or in a locked cupboard or desk.

CI that has been classified as CONFIDENTIAL or higher and needs to be transferred outside of the company must be sent via the CI registry. CI classified as CONFIDENTIAL MATERIAL – FOR OFFICIAL USE ONLY can be sent nationally as a normal letter or parcel.

It is prohibited for CI to be processed at home. Whenever CI is to be taken away on a trip, prior authorisation to do so must be obtained from the information security officer. CI that has been classified as TOP SECRET is not permitted to be taken away.

3.8. Use of information technology

The use of information technology (computers, fax machines, etc.) for processing and sending CI carries particular risk.

For this reason, special security measures have to be undertaken before CI classified as CONFIDENTIAL or higher can be processed or transmitted. The use

of information technology for CI of this level or higher must be expressly authorised by the Federal Ministry for Economic Affairs and Climate Action.

Electronic data carriers (discs, removable discs) provide CI to multiple users. Special rules apply to the labelling, deletion of data on, and destruction of data carriers of this kind. Ask your information security officer for more details.
Whenever information technology is used to process or transmit CI classified as CONFIDENTIAL MATERIAL – FOR OFFICIAL USE ONLY, the security measures set out on the information sheet on this level of CI must be observed.

4. What should I do when...?

Intelligence services, terrorist, and criminal organisations, as well as corporate rivals have many different methods of using particular persons to their own ends. Before a foreign intelligence service, for instance, approaches you and decides on how it is going to solicit your help, it will already have looked into who you are, what duties you perform or might perform in the future, what inclinations, desires, and habits you have, where your particular interests lie (theatre, free time, hobbies, etc.), what political views you hold, and whether you have any particular problems or weaknesses (financial difficulties, risk of bankruptcy, a lifestyle that is hard to maintain, etc.).

The results of their undercover research will dictate the method used by the intelligence service/other body to recruit you.

If an agent is commissioned with recruiting you, he or she will know all about you. He or she will know about your inclinations, weaknesses, desires, and habits.

Establishing contact with you will always appear to happen ‘by chance’, whether at a café or whilst you are on holiday, at an evening reception, at your front door, through a newspaper advert, or following a harmless exchange of letters. Before you are prompted to work for the body that is attempting to recruit you, the contact it has with you will have been maintained and cemented over a significant period of time – perhaps even years.

Agents often use a ruse to disguise who they really represent, i.e. they claim to work for a different body that is unsuspicious.

Just like foreign intelligence services, strangers, acquaintances, or even trusted persons might also approach you in order to pursue specific objectives connected with industrial espionage, espionage, or terrorism.

In order to avoid putting your colleagues, your company, or even the Federal Republic of Germany at risk, it is vital that you are able to recognise it early on if you become the target of this kind of contact.

If someone is more interested in your company than they are in you, then they are probably not a good friend. An acquaintance who does not respect that fact that you will not talk about matters on which security of information must be upheld, is not worthy of your respect.

Anyone who tries to persuade you to disclose confidential information or to ignore rules on CI to do them 'little favours' should be met with caution.

Try to get to the bottom of their behaviour towards you. Does your acquaintance truly desire contact with you, does he or she wish to be friends, or is he or she just looking for information?
If you are in doubt, or have any questions, do not hesitate to contact your information security officer and/or the Federal Office for the Protection of the Constitution in Cologne, or the authority responsible for protection of the constitution in your region. You do not lose anything by asking, but it can save you a lot of trouble. You may request for the information you provide to be dealt with confidentially. If you have already fallen into the clutches of intelligence services or are in a situation whereby you are betraying information in another way, you still have the opportunity to break out, without incurring significant personal damage. You can do this by approaching your information security officer or the authorities tasked with protecting the constitution to voluntarily disclose information about what has been happening. Use this opportunity in your own best interest and take back control of your life.

5. Summary

It is not only the responsibility of the relevant authorities to protect the lives of your colleagues, give your company the opportunity to compete, and ensure the internal and external security of the Federal Republic of Germany. It is also the obligation of every single citizen. As a colleague who has authorised access to CI at your

company, you carry particular responsibility. You are therefore called to follow the rules on handling CI with utmost care, working in close cooperation with your information security officer and the Federal Ministry for Economic Affairs and Climate Action. Furthermore, should you become aware of anyone behaving in a way that contravenes these rules or take note of anything else of relevance (e.g. unfamiliar persons in control and exclusion zones, items of 'unattended' luggage, unexpected maintenance work on your telephone or PC, etc.), you must report this to your information security officer, who will deal with your information confidentially. This also applies to potential espionage conducted on your company by rivals or by terrorist organisations. Reckless conduct and false camaraderie causes risk and harm to everyone concerned, including you – putting your job, your security, and possibly even your health and your life in jeopardy.

6. An appeal to you

We call upon you to play your part in protecting the security of CI against different kinds of attack and espionage by foreign intelligence services so as to prevent irreparable damage to our economy. Remain circumspect and wary whenever consulting CI and keep all rules and instructions on protecting CI down to the letter. Recklessness, negligence, self-promotion, or the imprudent use of communication technology often lead to the loss of valuable information, which damages our economy, your company, and yourself. Please help prevent this from happening.

Note:

The following penal provisions, with the exception of Section 353 b subsection 2, apply to everybody, not just to those who have a special duty to maintain confidentiality.

7. Extract from the German Criminal Code:

Section 93

Definition of state secret

(1) State secrets shall be facts, objects or knowledge which are only accessible to a limited category of persons and must be kept secret from a foreign power in order to avert a danger of serious prejudice to the external security of the Federal Republic of Germany.

(2) Facts which constitute violations of the independent, democratic constitutional order or are kept secret from the treaty partners of the Federal Republic of Germany and constitute violations of international arms control agreements, shall not be state secrets.

Section 94

Treason

(1) Whosoever

1. communicates a state secret to a foreign power or one of its intermediaries; or

2. otherwise allows a state secret to come to the attention of an unauthorised person or to become known to the public in order to prejudice the Federal Republic of Germany or benefit a foreign power

and thereby creates a danger of serious prejudice to the external security of the Federal Republic of Germany, shall be liable to imprisonment of not less than one year.

(2) In especially serious cases the penalty shall be imprisonment for life or of not less than five years. An especially serious case will typically occur if the offender

1. abuses a position of responsibility which especially obliges him to safeguard state secrets; or

2. through the offence creates the danger of an especially serious prejudice to the external security of the Federal Republic of Germany.

Section 95

Disclosure of state secrets with intent to cause damage

(1) Whosoever allows a state secret which has been kept secret by an official authority or at its behest to come to the attention of an unauthorised person or become known to the public, and thereby creates the danger of serious prejudice to the external security of the Federal Republic of Germany, shall be liable to imprisonment from six months to five years unless the offence is punishable under section 94.

(2) The attempt shall be punishable.

(3) In especially serious cases the penalty shall be imprisonment from one to ten years. Section 94 subsection 2 sentence 2 shall apply.

Section 96

Treasonous espionage; spying on state secrets

(1) *Whosoever obtains a state secret in order to disclose it (section 94) shall be liable to imprisonment from one to ten years.*

(2) *Whosoever obtains a state secret which has been kept secret by an official agency or at its behest in order to disclose it (section 95) shall be liable to imprisonment from six months to five years. The attempt shall be punishable.*

Section 97

Disclosure of state secrets

(1) *Whosoever allows a state secret which has been kept secret by an official agency or at its behest to come to the attention of an unauthorised person or become known to the public, and thereby negligently causes the danger of serious prejudice to the external security of the Federal Republic of Germany, shall be liable to imprisonment not exceeding five years or a fine.*

(2) *Whosoever recklessly allows a state secret which has been kept secret by an official agency or at its behest and which was accessible to him by reason of his public office, government position or assignment given by an official authority, to come to the attention of an unauthorised person, and thereby negligently causes the danger of serious prejudice to the external security of the Federal Republic of Germany, shall be liable to imprisonment not exceeding three years or a fine.*

(0) .....

Section 97a

Disclosure of illegal secrets

Whosoever communicates a secret, which is not a state secret because of one of the violations indicated in section 93 subsection 2, to a foreign power or one of its intermediaries and thereby creates the danger of serious prejudice to the external security of the Federal Republic of Germany, shall be punished as if he had committed treason (section 94). Section 96 subsection 1, in conjunction with section 94 subsection 1 number 1 shall apply mutatis mutandis to secrets of the kind indicated in sentence 1.

Section 97b

Disclosure based on mistaken assumption that secret is illegal

(1) *If the offender in cases under sections 94 to 97 mistakenly assumes that a state secret is a secret of the kind indicated in section 97a he shall be punished pursuant to the those provisions if*

1. *he could have avoided the mistake;*
2. *he did not act with the intention ofpreventing the alleged violation; or*
3. *the act is, under the circumstances, not an appropriate means to accomplish that purpose.*

The act is typically not an appropriate means if the offender did not previously seek a remedy from a member of the Federal Parliament.

(2) If the state secret was confided or made accessible to the offender in his capacity as a public official or soldier in the Armed Forces he shall also incur liability if he did not previously seek a remedy from a superior in government service, or in the case of a soldier from a superior disciplinary officer. This shall apply mutatis mutandis to persons entrusted with special public service functions and to persons under a duty within the meaning of section 353b subsection 2.

Section 98

Treasonous activity as an agent

(1) Whosoever

1. *engages in activity for a foreign power which is directed towards the acquisition or communication of state secrets; or*
2. *declares to a foreign power or one of its intermediaries his willingness to engage in such activity,*

shall be liable to imprisonment not exceeding five years or a fine unless the offence is punishable pursuant to section 94 or section 96 subsection 1. In especially serious cases the penalty shall be imprisonment from one to ten years; section 94 subsection 2 sentence 2 number 1 shall apply mutatis mutandis.

(2) The court in its discretion may mitigate the sentence (section 49 subsection 2) or order a discharge under these provisions if the offender voluntarily gives up his activity and discloses his knowledge to a government authority. If the offender in cases under subsection 1 sentence 1 above has been forced into the activity by the foreign power or one of its intermediaries, he shall not be liable under this provision if he voluntarily gives up his activity and discloses his knowledge to a government authority without unnecessary delay.

Section 99

Working as an agent for an intelligence service

(1) Whosoever

1. *engages in intelligence activity for the intelligence service of a foreign power against the Federal Republic of Germany which is directed toward communication or supply offacts, objects or knowledge, or*
2. *declares to the intelligence service of a foreign power or one of its intermediaries his willingness to engage in such activity,*

shall be liable to imprisonment not exceeding five years or a fine unless the offence is punishable under section 94, section 96 subsection 1, section 97a, or section 97b in conjunction with section 94 or section 96 subsection 1.

(2) In especially serious cases the penalty shall be imprisonment from one to ten years. An especially serious case typically occurs if the offender communicates or supplies facts, objects or knowledge which have been kept secret by an official agency or at its behest, and he

1. *abuses a position of responsibility which especially mandates him to safeguard such secrets; or*
2. *through the offence creates the danger of serious prejudice to the Federal Republic of Germany.*

(3) Section 98 subsection 2 shall apply mutatis mutandis.

Section 353b

Breach of official secrets and special duties of confidentiality

Whosoever unlawfully discloses a secret which has been confided or become known to him in his capacity as

1. *a public official;*
2. *a person entrusted with special public service functions; or*
3. *a person who exercises duties or powers under the laws on staff representation*

and thereby causes a danger to important public interests, shall be liable to imprisonment not exceeding five years or a fine. If by the offence the offender has negligently caused a danger to important public interests he shall be liable to imprisonment not exceeding one year or a fine.

(2) Whosoever other than in cases under subsection 1 above unlawfully allows an object or information to come to the attention of another or makes it publicly known

1. *which he is obliged to keep secret on the basis of a resolution of a legislative body of the Federation or a state or one of their committees; or*
2. *which he has been formally put under an obligation to keep secret by another official agency under notice of criminal liability for a violation of the duty of secrecy,*

and thereby causes a danger to important public interests shall be liable to imprisonment not exceeding three years or a fine.

(3) The attempt shall be punishable.

(4)

Extract from the German Code of Criminal Procedure

Section 153e

Dispensing with Court Action in cases of active remorse

(1) If criminal offences of the nature designated under section 74a subsection 1, numbers 2 to 4, and section 120 subsection 1 numbers 2 to 7, of the Courts Constitution Act are the subject of the proceedings, the Federal Public Prosecutor General, with the approval of the Higher Regional Court competent pursuant to section 120 of the Courts Constitution Act, may dispense with prosecuting such an offence if the perpetrator, subsequently to the offence, and before he has learned of the discovery thereof, contributed towards averting a danger to the existence or the security of the Federal Republic of Germany or its constitutional order. The same shall apply if the perpetrator has made such

contribution by disclosing to an agency after the offence such knowledge as he had with respect to endeavours involving high treason, endangering the democratic state based on the rule of law, treason, and endangering external security.

(2) If charges have already been preferred, the Higher Regional Court competent pursuant to section 120 of the Courts Constitution Act may, with the approval of the Federal Public Prosecutor General, terminate the proceedings if the conditions designated under subsection 1 are met.