Directive 2009/81/EC on the award of contracts in the fields of defence and security

Guidance Note
Security of Information

Directorate General Internal Market and Services

1) Introduction

1. Given the sensitive nature of many defence and security procurements, Security of Information is a particularly important feature of Directive 2009/81/EC.[1] The ability and the reliability of economic operators to protect classified information[2] are indeed crucial for the award and execution of many defence and sensitive security contracts. Security of Information requirements are on-going during the lifetime of a contract and will be practically tested during contract execution.

At the same time, the openness of defence and security markets in the EU is hampered by the absence of an EU-wide regime for Security of Information. It is up to each Member State to determine which information is to be classified at which level of confidentiality, and each Member State grants its own national security clearances certifying a supplier's capacity to protect classified information. These security clearances are not automatically recognised by other Member States. In many cases, however, bilateral or other appropriate security agreements or arrangements include provisions concerning the mutual recognition of security clearances, which alleviates the negative impact on the effectiveness of the Directive.

2. The Directive provides for various safeguards concerning Security of Information, which should make it possible for contracting authorities/entities to limit both exclusions and Treaty-based exemptions on the grounds of confidentiality to really exceptional cases.

Security of Information appears at different places in the Directive: it is mentioned as a requirement for the tendering and contracting phase (Article 7), and can be a cause for exclusion (Article 13), a contract condition (Articles 20 and 22), and a selection criterion (Article 39 and 42). Taken in combination, these provisions allow requirements for the protection of classified information to be applied throughout all phases from the beginning of the contract award procedure until the end of contract execution.

---

1 See recitals 8 and 9 of the Directive.

2 According to Article 1(8) of the Directive, classified information '*means any information or material, regardless of the form, nature or mode of transmission thereof, to which a certain level of security classification or protection has been attributed, and which, in the interests of national security and in accordance with the laws, regulations or administrative provisions in force in the Member State concerned, requires protection against any misappropriation, destruction, removal, disclosure, loss or access by any unauthorised individual, or any other type of compromise*'.

2) General provisions: Protection of classified information

3. Article 7 is part of the general principles for the conduct of the procedure. It allows contracting authorities/entities to '*impose on economic operators requirements aimed at protecting the classified information they communicate throughout the tendering and contracting procedure. They may also request these economic operators to ensure compliance with such requirements by their subcontractors'*.

This provision ensures the security of classified information passed from contracting authorities/entities to all candidates and tenderers until the actual award of the contract. In practice, Article 7 allows the contracting authority/entity to make any participation in the procedure, in particular the dispatch of contract documents to selected candidates, subject to the (pre-contractual) commitment of candidates/tenderers to safeguard appropriately all classified information brought to their knowledge and/or to provide, if necessary, a specific security clearance.

4. Once the contract is awarded, the appropriate degree of Security of Information can be ensured by contract performance conditions under Articles 20 and 22 of the Directive.

3. Criteria for qualitative selection

3.1) General principles

5. Articles 39 to 46 of the Directive deal with the qualitative selection of candidates and tenderers. At this stage of the procedure, the contracting authority/entity has to assess the suitability of economical operators on the basis of exclusion criteria and criteria relating to economic and financial standing and professional and technical knowledge or ability. In defence and sensitive security contract awards, reliability and the ability to guarantee security of information is one of the key criteria for qualitative selection.

The qualitative selection of candidates and tenderers is to be distinguished from the assessment of tenders in the contract award phase. It is strictly limited to the suitability of the economic operators and concerns therefore only their standing, ability and reliability as such, not the products and services they propose for execution of the contract.

6. In restricted procedures, negotiated procedures with publication of a contract notice and competitive dialogues, qualitative selection normally takes place at the moment of the selection of candidates to be invited to submit a tender. Article 38(3) of the Directive provides that *'contracting authorities/entities may limit the number of suitable candidates they will invite to tender or with which they will conduct a dialogue'* by using objective and non-discriminatory selection criteria.

In addition, contracting authorities/entities can require candidates to meet certain minimum capacity levels defined in accordance with Articles 41 and 42 of the Directive.

3.2) Grounds for exclusion of candidates and tenderers

7. Article 39 contains a list of cases where a candidate or tenderer may be excluded from participation in a contract award procedure. While the first paragraph provides for mandatory exclusion in the case of convictions by final judgment for certain offences, the second paragraph gives the contracting authority a margin of discretion in its decision to exclude candidates or tenderers who have committed specific forms of professional misconduct. According to ECJ case-law, the lists of grounds for exclusion in Article 39(1) and (2) are exhaustive. It would therefore not be possible for Member States or contracting authorities/entities to exclude candidates or tenderers on the basis of other criteria relating to their professional qualities.[3]

Article 39(2) contains two exclusion criteria related to Security of Information. It provides that *'any economic operator may be excluded from participation in a contract where that economic operator:*

...

(d) has been guilty of grave professional misconduct proven by any means which the contracting authority/entity can supply, such as a breach of obligations regarding security of information or security of supply during a previous contract;

(e) has been found, on the basis of any means of evidence, including protected data sources, not to possess the reliability necessary to exclude risks to the security of the Member State'.

8. Point (d) refers explicitly to breaches of Security of Information obligations during previous contracts. This also covers breaches of such obligations vis-à-vis other contracting authorities/entities, no matter in which Member State they are established. Although the provision does not require a conviction by final judgment, the rather strong terms '*has been guilty'* and '*proven'* indicate that the contracting authority/entity has to rely on objective and verifiable information if it wants to exclude a candidate/tenderer from the procedure on these grounds.

9. Point (e) deals with the reliability of candidates and tenderers. Recital 67 confirms that '*given the sensitive nature of the defence and security sectors, the reliability of economic operators to which contracts are awarded is vital. This reliability depends, in particular, on their ability to respond to requirements imposed by the contracting authority/entity with respect to security of supply and security of information'*. Recital 65 broadens the concept of reliability, specifying that economic operators must be '*sufficiently reliable so as to exclude risks to the security of the Member State. Such risks could derive from certain features of the products supplied or from the shareholding structure of the candidate'*. This confirms that the reliability of economic operators may also depend on factors other than their ability to protect classified information.

[3] Judgment of 16 December 2008 in Case C-213/07 Michaniki AE, paragraph 43.

In view of the particular sensitivity of certain defence and security contracts, Article 39(2)(e) allows to demonstrate the lack of reliability '*by any means of evidence, including protected data sources*'. Recital 65 specifies that *'it should ... be possible to exclude economic operators if the contracting authority/entity has information, where applicable provided by protected sources, establishing that they are not sufficiently reliable so as to exclude risks to the security of the Member State'*.

Point (e) and recital 65 point to cases where contracting authorities/entities may question the reliability of a candidate even when it holds security clearances from its national authorities. In these cases, which go well beyond purely legal or normal procurement issues, protected data sources may indeed be an important — if not the only — means to establish that security risks cannot be excluded.

However, point (e) does not give unlimited discretion to contracting authorities/entities. Any exclusion of a candidate or tenderer must be based on risks to the security of the Member State. Moreover, subject to Article 346(1)(a) TFEU, the contracting authority/entity must still be prepared to demonstrate, if necessary in a special review procedure, the plausibility of its decision.

3.3) Criteria of technical and/or professional ability

10. Article 42(1) describes different means by which economic operators may furnish evidence of their technical abilities. Contracting authorities/entities can use these means as a basis for their selection criteria.

According to Article 38, contracting authorities/entities may use selection criteria in two ways:

- First, they may require candidates to meet minimum capacity levels. *'The extent of the information (…) and the minimum levels of ability required for a specific contract must be related and proportionate to the subject-matter of the contract*.'
- Second, they can use them as basis for drawing up a ranking if they decide to limit the number of suitable candidates they will invite to tender.

11. In the context of Security of Information, point (j) of Article 42(1) is particularly important. It requires *'in the case of contracts involving, entailing and/or containing classified information, evidence of the ability to process, store and transmit such information at the level of protection required by the contracting authority/entity. In the absence of harmonisation at Community level of national security clearance systems, Member States may provide that this evidence has to comply with the relevant provisions of their respective national laws on security clearance.'*

In this context, recital 68 specifies that *'… it is for the contracting authorities/entities or Member States to define the level of technical capacity which is required in this regard for participation in an award procedure and to assess whether candidates have achieved the required security level'.*

The only evidence of a candidate's ability to handle classified information at the level of protection required is a facility security clearance granted by its own National/Designated Security Authorities under the relevant national rules. These facility security clearances are issued only for contracts involving classified information at the level of CONFIDENTIAL or above (not for RESTRICTED). In this context, it is important to note that economic operators do not possess a copy of this security clearance. Contracting authorities/entities can therefore only require from candidates a statement that they hold such a clearance or that they are prepared to take the necessary security measures to obtain such a clearance. Contracting authorities/entities shall then contact the competent National/Designated Security Authorities to obtain confirmation that the candidate holds a facility security clearance at the required level or, where appropriate, to request that the security clearance procedure for the candidate is initiated.

12. According to recital 43, '*it is for the contracting authorities/entities or Member States … to determine whether they consider security clearances issued in accordance with the national law of another Member State as equivalent to those issued by their own competent authorities'*. At the same time, however, Article 42(1)(j) specifies that '*Member States shall recognise security clearances which they consider equivalent to those issued in accordance with their national law, notwithstanding the possibility to conduct and take into account further investigations of their own, if considered necessary'.* In many cases, Member States have bilateral security agreements or arrangements concerning the equivalence of security classifications and security requirements, such as security clearances for a company's facilities or personnel. In such cases, contracting authorities/entities shall accept security clearances granted by National/Designated Security Authorities of another Member State as evidence of a candidate's capacity to ensure the security of classified information in accordance with national security laws and regulations and the bilateral agreements or arrangements.

However, '*even where such agreements* [or arrangements] *exist, the capacities of economic operators from other Member States as regards security of information can be verified, and such verification should be carried out in accordance with the principles of non-discrimination, equal treatment and proportionality*' (recital 68). Such verification can normally be performed only by the National/Designated Security Authority of the Member State in which the economic operator is located. Accordingly, the fourth subparagraph of Article 42(1)(j) specifies that '*the contracting authority/entity may ask the national security authority of the candidate's Member State or the security authority designated by that Member State to check the conformity of the premises and facilities that may be used, the industrial and administrative procedures that will be followed, the methods for managing information and/or the situation of staff likely to be employed to carry out the contract'.*

The third subparagraph of Article 42(1)(j) provides that *'the contracting authority/entity may, where appropriate, grant candidates which do not yet hold security clearance additional time to obtain such clearance. In this case, it shall indicate this possibility and the time-limit in the contract notice'.* In order to improve market access for newcomers and to broaden the defence and security supplier base to include non-established

players, contracting authorities/entities should make use of this possibility wherever this is possible without hampering the award procedure.

13. In practical terms, contracting authorities/entities may use as a selection criterion the ability of candidates to process, store and transmit classified information related to the contract at the required level of protection. The only evidence for this ability will be security clearances granted by the national authority of the Member State where the candidate (and/or its relevant facilities) is established. On that basis, it is difficult to establish minimum requirements or rankings: the question is merely whether these clearances are recognised or not. If the Member States where the contracting authority/entity and the candidate are located have a bilateral agreement or arrangement on Security of Information, clearances will normally be recognised automatically, though possibly subject to further investigation, if considered necessary. In the absence of such bilateral agreements or arrangements, contracting authorities/entities are not formally obliged to recognise security clearances. However, in their decision to take this as a reason to exclude or not a candidate or tenderer from another Member State, they have to comply with the principal of proportionality in order to limit market access market access restriction to the strict minimum.

In this context, it is important to note that a security clearance *per se* does not grant the right to receive classified information – it is a precondition for the person or authority who holds the classified information to release it to the company or person who holds the clearance. Even to a security-cleared receiver, classified information is released only on a need-to-know basis, and only if no other security reasons stand against it. This is where reliability comes into play: As a general rule, Member States should consider a national security clearance issued by another Member State as sufficient evidence for the reliability of a company. However, the Directive makes it clear that other factors may be taken into account as well and therefore mentions reliability as a separate selection criterion. Since reliability is a vague concept, contracting authorities/entities have both a considerable degree of flexibility for their assessment, but also a special responsibility to handle it with care. If it is used as a criterion, they will normally not do the assessment themselves, but ask their National/Designated Security Authorities whether there are elements indicating a possible lack of reliability of a candidate or tenderer.

4) Conditions for performance of the contract

4.1) Principles

14. According to Article 20 of the Directive, *'contracting authorities/entities may lay down special conditions relating to the performance of a contract, provided that these are compatible with Community law and are indicated in the contract documentation'.* These conditions may, in particular, seek to ensure *'the security of classified information required by the contracting authority/entity'*, in accordance with Article 22. Recital 41 notes that *'contract performance conditions are compatible with this Directive provided that they are not directly or indirectly discriminatory and are indicated in the contract*

notice or in the contract documents.' These conditions will typically take the form of contract clauses imposing specific obligations on the successful tenderer.

Recital 43 specifies that *'in order to ensure security of information, contracting authorities/entities may require in particular commitments from both contractors and subcontractors to protect classified information against unauthorised access, as well as sufficient information regarding their capacity to do so. In the absence of a Community regime on security of information, it is for the contracting authorities/entities or Member States to define these requirements in accordance with their national laws and regulations, and to determine whether they consider security clearances issued in accordance with the national law of another Member State as equivalent to those issued by their own competent authorities'*.

15. From a procedural point of view, it is important for the contracting authority/entity to provide all tenderers with a sound basis for the preparation of their tenders and to inform them comprehensively and in time of its Security of Information requirements and how to meet them. The contracting authority/entity must therefore include in the contract notice at least a comprehensive list of all its Security of Information requirements, and then spell out in detail in the contract documents (or in the accompanying descriptive or supporting documents):

- the content of the Security of Information obligations under the contract, and
- the particulars (commitments, information) to be submitted in the tender in order to demonstrate that the Security of Information requirements are met.

16. The second subparagraph of Article 22 contains a non-exhaustive list of particulars that the contracting authority/entity may require to be included in the tender. In this context, specific commitments to safeguard all classified information related to the contract are particularly important. The third subparagraph specifies that Member States may provide that these commitments *'have to comply with their national provisions on security clearance'.*

4.2) Commitment to safeguard confidentiality

Article 22
…
(a) a commitment from the tenderer and the subcontractors already identified to appropriately safeguard the confidentiality of all classified information in their possession or coming to their notice throughout the duration of the contract and after termination or conclusion of the contract, in accordance with the relevant laws, regulations and administrative provisions;

(b) a commitment from the tenderer to obtain the commitment provided in point (a) from other subcontractors to which it will subcontract during the execution of the contract;

17. Points (a) and (b) of Article 22 provide a useful complement to the selection criterion in Article 42(j). While the latter allows the candidate's general ability to safeguard classified information at the required level to be verified on the basis of security clearances, the contract execution condition makes it possible to get a firm commitment, underpinned by security clearances, to use this ability to protect the concrete information received in relation with the contract. Such a commitment can be required not only from the tenderer but also from subcontractors. The two provisions thus form a coherent system that allows the contracting authority/entity to ensure firstly that only reliable operators possessing the necessary abilities are invited to tender and secondly that they undertake to ensure adequate protection of classified information.

> *…*
>
> *(c) sufficient information on subcontractors already identified to enable the contracting authority/entity to determine that each of them possesses the capabilities required to appropriately safeguard the confidentiality of the classified information to which they have access or which they are required to produce when carrying out their subcontracting activities;*
>
> *(d) a commitment from the tenderer to provide the information required under point (c) on any new subcontractor before awarding a subcontract.*

18. Points (c) and (d) add a further element to the system for the protection of classified information: the contracting authority/entity may require tenderers to submit information on their subcontractors so that it can verify their ability to safeguard the classified information made available to them. In practice, this information may consist of certificates from their National/Designated Security Authority confirming that the subcontractors concerned hold national clearances at the necessary security level. Contracting authorities/entities may then check this information with the competent National/Designed Security Authorities. They are thus able to verify the reliability of not only the main contractor but the subcontractors as well.

5. Procedural aspects

5.1) Information for unsuccessful candidates and tenderers

19. Article 35(1) of the Directive provides that *'the contracting authorities/entities shall, at the earliest opportunity, inform candidates and tenderers of decisions reached concerning the award of a contract … including the grounds for any decision not to award a contract…'*. In addition, the contracting authority/entity must, upon written request, inform unsuccessful candidates or tenderers of the reasons for their rejection,

including, *'in the cases referred to in Articles 22 and 23, the reasons for its decision of non-conformity with the requirements of security of information and security of supply'*.

20. This information obligation results from the principle of transparency. It is crucial as a guarantee for the fairness of the procedure and, at the same time, a necessary precondition for meaningful exercise of the right of judicial protection. However, full transparency of the reasons for the exclusion of a candidate or the rejection of a tender might conflict with the security of classified information, especially when such decisions are based on information from protected sources.

In such cases, Article 35(3) allows contracting authorities/entities to *'withhold certain information on the contract award … where release of such information would impede law enforcement or otherwise be contrary to the public interest, in particular defence and/or security interests…'.* If these conditions are met, the contracting authority/entity may therefore decide not to communicate information, even if this means that the candidate or tenderer cannot be informed of the main reason for its rejection. However, the candidate or tenderer concerned would remain free to challenge the rejection in a review procedure.

5.2) Requirements for review procedures

21. The same conflict exists when an unsuccessful candidate or tenderer files for review of its rejection under the procedure provided for in Articles 54 to 64 of the Directive. Under Article 55(2), Member States have to ensure that decisions taken by the contracting authorities/entities may be reviewed effectively *'on the grounds that such decisions have infringed Community law in the field of procurement …'.* This applies first and foremost to decisions to exclude candidates from the procedure or to reject tenders.

The contracting authority/entity must therefore be prepared to state the reasons for its decisions before the review body. This also applies in cases where it was allowed, under Article 35(3), to withhold certain information from the unsuccessful candidate or tenderer.

22. However, Article 56(10) sets out specific provisions to reconcile the basic principle of effective judicial review with the specific need to protect classified information. It requires Member States to *'ensure that the bodies responsible for review procedures guarantee an adequate level of confidentiality of classified information or other information contained in the files transmitted by the parties, and act in conformity with defence and/or security interests throughout the procedure'.* To this end, Member States may decide to assign responsibility for the review of contracts in the fields of defence and security to a specific review body.

The third subparagraph of Article 56(10) specifies further that *'Member States may provide that only the members of review bodies personally authorised to deal with classified information may examine applications for review involving such information.*

They may also impose specific security measures concerning the registration of applications for review, the reception of documents and the storage of files'.

Such measures should ensure that contracting authorities/entities can communicate all classified information to the review body without running the risk of undue disclosure. However, these measures cannot completely resolve the basic conflict inherent in the conduct of such review proceedings: On the one hand, the applicant must know the reasons for the decision in order to obtain effective judicial protection of its rights and to put forward its arguments. On the other hand, communication of these reasons might be incompatible with the required protection of classified information.

23. The Directive leaves it to the Member States to develop adequate solutions to this dilemma within their national legal frameworks. The fourth subparagraph of Article 56(10) states merely that *'Member States shall determine how review bodies are to reconcile the confidentiality of classified information with respect for the rights of the defence, and, in the case of a judicial review or of a review by a body which is a court or tribunal … , shall do so in such a way that the procedure complies, as a whole, with the right to a fair trial.'*

6) Security of Information: specific exclusions and Treaty-based derogations

6.1) Article 13(a): Disclosure of information

24. According to Article 13(a), the Directive does not apply to '*contracts for which the application of the rules of this Directive would oblige a Member State to supply information the disclosure of which it considers contrary to the essential interests of its security'*. This exclusion is based on Article 346(1)(a) TFEU, which states that '*no Member State shall be obliged to supply information the disclosure of which it considers contrary to the essential interests of its security*'. The main difference is that the text of Article 346(1)(a) TFEU mentions only the right not to disclose information but no further measures possibly related to such non-disclosure. Article 13(a), by contrast, establishes an explicit link between non-disclosure of information and non-application of the Directive. This specification seems particularly important for contracts awarded in the field of non-military security, which are not covered by Article 346(1)(b) TFEU.

25. Recital 27 explains which contracts are covered by the exclusion in Article 13(a), namely '*contracts which are so sensitive that it would be inappropriate to apply this Directive, despite its specificity*'. Recital 27 also mentions security areas that are particularly sensitive, and where procurements may therefore often be highly confidential. This is the case for '*particularly sensitive purchases which require an extremely high level of confidentiality, such as, for example, certain purchases intended for border protection or combating terrorism or organised crime, purchases related to encryption or purchases intended specifically for covert activities or other equally sensitive activities carried out by police and security forces*'.

This list is only indicative and refers to '*certain purchases*'. This means that not all contracts awarded in these areas are automatically covered by the exclusion provided for in Article 13(a), but also that equally sensitive cases may arise in other security areas as well. However, the list in recital 27 also indicates that Article 13(a) was introduced essentially to allow for the explicit exclusion of highly confidential non-military security contracts.

26. In any case, Article 13(a) must be applied in the light of Article 11, which is a general safeguard clause against the use of Articles 12 and 13 for the purpose of avoiding transparent and competitive contract award procedures. Under ECJ case-law, provisions that authorise exceptions to EU public procurement rules must be interpreted strictly.[4] This means that the exclusions under Articles 12 and 13 must be confined to contracts of the type described in these provisions. The burden of proving that a contract comes under one of the exclusions listed in Article 12 and 13 lies on the contracting authority/entity seeking to use it. Moreover, the principle of proportionality as described below under 6.3) in the context of Article 346 TFEU applies to Article 13(a) as well. This is particularly important since the reasoning for using the Article 13(a) exclusion and the Treaty-based exemption may often be very similar.

6.2) Article 13(b): Contracts for the purposes of intelligence activities

27. Article 13(b) provides a tailor-made exclusion for a specific category of highly sensitive contracts, namely '*contracts for the purposes of intelligence activities*'. According to recital 27, this includes '*procurements provided by intelligence services, or procurements for all types of intelligence activities, including counter-intelligence activities, as defined by Member States*'. This provision is based on the assumption that contracts related to intelligence are by definition too sensitive to be awarded in a transparent and competitive procedure. It covers both cases where other public authorities award contracts to intelligence services, for specific supplies, works or services (e.g. protection of government IT networks), and cases where intelligence services award contracts for the purpose of their intelligence activities.

28. Article 13(b) refers to intelligence activities, not to intelligence services or agencies. Moreover, recital 27 leaves it to Member States to define 'intelligence activities, including counter-intelligence activities'. The legislator chose this approach mainly for two reasons. First, not all purchases made by intelligence services are necessarily so sensitive that EU procurement rules cannot be applied; consequently, the exclusion covers only those purchases made for the purposes of intelligence activities. Second, there is no single commonly agreed definition of intelligence, and the way intelligence activities are organised differs between Member States. The definition of the scope of Article 13(b) takes this diversity into account and covers purchases for the purpose of all types of intelligence activities, no matter whether the service or agency concerned is in charge of a specific intelligence function (military, security, criminal or external

[4] See judgment of 13 December 2007 in Case C-337/06 Bayerischer Rundfunk, paragraph 64.

intelligence) or specialised in the collection of information from certain sources (e.g. imagery or signals intelligence).

6.3) Security of information under Article 346 TFEU

29. According to recital 16, Article 346 TFEU covers '*contracts in the fields of both defence and security … which are so confidential … that even the specific provisions of this Directive are not sufficient to safeguard Member States' essential security interests*'. Recital 20 specifies that Article 346(1)(a) TFEU in particular '*gives Member States the possibility to exempt contracts in the fields of both defence and security from the rules of this Directive if the application of this Directive would oblige them to supply information, the disclosure of which they consider contrary to the essential interests of their security ...'.*

30. According to established ECJ case-law, the derogation under Article 346 TFEU is limited to exceptional and clearly defined cases and must not be used beyond the limits of such cases. Like any other derogation from fundamental freedoms, it has to be interpreted strictly.[5]

Therefore, the decision to rely on Article 346 TFEU has to be based on a case-by-case assessment, taking into account the principle of proportionality and the need for a strict interpretation of Article 346 TFEU. In the context of Security of Information, the key questions for contracting authorities/entities are:

- Which information cannot be disclosed?
- To whom can the information not be disclosed?

Whatever the answers to these questions are – Member States will if necessary have to be able to demonstrate that the restriction they impose is appropriate and proportional for the protection of their essential security interests. This implies that contracting authorities/entities always have to ensure that they apply the least restrictive measure necessary for the protection of national security interests.

31. The most restrictive approach is not to disclose any information at all on a contract. These extreme cases may be necessary for contracts which '*are so sensitive that their very existence must be kept secret'* (recital 20)*.* Here, even the simple publication of a voluntary ex ante notice, contract notice or contract award notice could put at risk essential security interests.

32. Less extreme cases are contracts for which contracting authorities/entities require that all members of the staff involved in the execution of the contract have personal security clearances and are citizens of the procuring Member State. In this case, the security clearances of other Member States are not considered to be sufficient safeguards for the protection of classified information. Such a 'national eyes only'

[5] See judgment in Case C-414/97 Commission v Spain, paragraph 22, and judgments of 15 December 2009, for instance Case C-239/06, paragraph 68.

condition infringes the principle of non-discrimination on the ground of nationality and can therefore also be justified only on the basis of Article 346 TFEU.

However, 'national eyes only' restrictions do not by definition exclude the possibility to use competitive procedures with EU-wide publication, in particular since these restrictions often apply only to certain aspects of contract performance. This may happen, for example, when highly sensitive devices are to be integrated in a larger system or equipment is to be installed in a highly restricted area. In these cases, contracting authorities can, depending on the level of integration and overlap,

- award the contract as a whole following one of the procedures of the Directive, but include a specific contract condition — justified on the basis of Article 346 TFEU — which requires the successful tenderer to involve only nationals with the appropriate security clearances in the execution of a particular part of the contract, or
- procure, if possible, the works, supplies or services subject to the 'national eyes' restriction under a separate contract. The main contract would then be awarded under full application of all the provisions of the Directive, while the separate contract would also be awarded following the procedure of the Directive, but include a 'national-eyes only' condition', to be justified on the basis of Article 346 TFEU.

33. In all these cases, Member States must always be able to demonstrate that the non-disclosure of information was appropriate to protect their essential security interests and to explain why it was not possible to achieve the same objective by less restrictive means. In other words: priority should always be given to the least restrictive solution.

This guidance note reflects the views of the services of DG MARKT and is legally not binding. Only the Court of Justice is competent to give a legally binding interpretation of EU law.