RADA
UNII EUROPEJSKIEJ

Bruksela, 5 czerwca 2009 r. (15.06)
(OR. en)

10715/09

LIMITE

CSC 20

NOTA

Od:	Sekretariat Generalny Rady
Do:	Komitet ds. Bezpieczeństwa
Nr poprz. dok.:	9518/08
Dotyczy:	Projekt decyzji Rady w sprawie zasad bezpieczeństwa dotyczących ochrony informacji niejawnych UE – wersja skonsolidowana

1. Following the meeting of the Security Committee on 28-29 May 2009, delegations will find attached a revised version of the draft Council Decision on the security rules for protecting EUCI resulting from the partial third reading by the Committee, and taking account of a number of additional comments received from delegations.

2. Draft declarations by the Council and by the Council and the Commission are set out in doc. 9518/09 ADD 1.

3. The Committee will undertake its final reading of the draft Council Decision, including all the Annexes and the draft declarations, at its meeting on 24 to 26 June 2009. As the Committee has now reached the final stages of its work, delegations are requested to come to that meeting fully prepared to settle the outstanding issues so that the Committee is in a position to report to COREPER in early July.

4. A number of delegations consider that the draft is acceptable as it stands and have appealed for delegations to refrain from making any further changes which might upset the overall balance of the contents.

5. In order to facilitate discussions at the meeting, delegations will find below some explanations on key issues revised at the last meeting and on the main outstanding issues.

Obligations for Member States deriving from the Council security rules

6. The Committee has examined extensively on several occasions the question of the obligations incumbent on Member States under the Council's security rules. The Committee acknowledges that the legal basis used (Article 207(3) of the TEC which is the basis for the Council's internal rules of procedure) does commit Member States to the extent required for the proper functioning of the Council. The Committee accordingly noted that:

– the formulation used in Article 1(2) of the draft ("*these basic principles and minimum standards shall… be respected by the Member States in accordance with their respective national laws and regulations*") is couched in balanced and neutral language as in the current security regulations, and reflects the common objective of ensuring that an equivalent level of protection is afforded to EUCI throughout the EU, with Member States taking all appropriate practical measures to achieve that result; for that reason it would be preferable to maintain the careful political balance struck in 2001;

– the phrase "*in accordance with their respective national laws and regulations*" in Article 1(2) makes it patently clear that Member States are not required to amend their national legislation on protecting classified information;

– the Council's security rules regulate only EU classified information and do not regulate the protection of national classified information under national law; with regard to the limited number of points in the Annexes addressed in detail by national law (e.g. the criteria used for security investigations on individuals (see Annex 1 paragraphs 8 and 9)), the wording has been particularly carefully chosen to ensure that no incompatibility with national law can arise; and

– no actual difficulties or incompatibilities have arisen in practice with regard to implementing the current security rules since 2001; all delegations and the GSC are committed to finding solutions to any difficulties which might arise in implementing the security rules by taking any practical measures required in a spirit of pragmatism and loyal cooperation.

These points will be reflected in the report to COREPER

Security classification markings

7. The Committee is invited to settle at its level at the June meeting the security classification markings to be used for EUCI, on the basis of security and technical considerations. The various positions presented to date are set out in the footnote to Article 2(2).

8. Reservations exist on abbreviated classification markings (Annex IV, paragraph 13), subject to final decision on Article 2(2).

Accreditation of systems handling RESTREINT UE

9. In order to address reservations by some delegations on the accreditation of CIS handling RESTREINT UE, the specific requirements, scale and degree of detail of the accreditation process have been covered in a new paragraph 7 in Annex III. A new paragraph 36 has also been inserted in Annex V regarding the accreditation of RESTREINT UE systems in industrial activities.

Technical security guidelines on RESTREINT UE

10. The substance of former Article 3(4) (technical security guidelines on the protection of RESTREINT UE information) will be mentioned in the note which will accompany the draft Decision to COREPER and Council and be included as a priority in the Committee's programme for future work.

Carriage of EUCI on electronic media protected by cryptographic products

11. Article 10(4)(b)(i) has been amended to better explain that, during carriage of EUCI on electronic media protected by cryptographic products, both the medium and its contents (i.e. the cryptogram) can be handled and stored as unclassified material. This is also covered in a new paragraph 23 in Annex II. A definition of "cryprogram" has been inserted in Appendix A.

FSC and PSC

12. The Committee will be invited to take a final view on the FSC requirement as set out in Article 11(5) and Annex V. The current wording provides that an FSC is required for contractors and sub-contractors handling EUCI classified CONFIDENTIEL UE or above "within their facilities". This would not undermine any obligation under national laws and regulations for an FSC to be issued to contractors and sub-contractors which are NOT required to handle such information within their facilities.

Handling and storage of EUCI at different classification levels

13. The Committee will be invited to take a final view on the provisions regarding areas in which EUCI may be handled and stored, in the light of the changes which were agreed at the last meeting.

Registration

14. On Annex IV, paragraph 18, regarding the classification level as from which registration for security purposes is required, two delegations consider that such requirement should only apply to information classified SECRET UE and above.

15. With regard to Annex IV, paragraph 21, one delegation considers that the requirement for the holder to sign a receipt should only apply to information classified SECRET UE and above.

Handling of EUCI by EU and EC agencies, bodies and offices

16. The Committee will be invited to take a view on the approach to EU and EC agencies, bodies and offices set out in the draft declaration in the addendum to this note (doc. 9518/09 ADD 1).

Definition of 'information'

17. In security of information agreements currently in force between the EU and third States or international organisations, "information" is defined as "knowledge that can be communicated in any form". This is the definition to be found in Appendix A.

Definition of 'originator'

18. The Committee will be invited to take a view on whether a definition of 'originator' should be included in the Decision and, if so, to agree on the wording to be included in Appendix A.

Projekt

DECYZJA RADY

z dnia xx 2009 r.

w sprawie zasad bezpieczeństwa dotyczących ochrony informacji niejawnych UE

(2009/xxx/WE)

RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat ustanawiający Wspólnotę Europejską, w szczególności jego art. 207 ust. 3,

uwzględniając decyzję Rady 2006/683/WE, Euratom z dnia 15 września 2006 r. w sprawie przyjęcia regulaminu wewnętrznego Rady[1], w szczególności jej art. 24,

a także mając na uwadze, co następuje

(1) Aby rozwinąć działania Rady we wszystkich dziedzinach wymagających pracy z wykorzystaniem informacji niejawnych, właściwe jest utworzenie kompleksowego systemu bezpieczeństwa służącego ochronie informacji niejawnych, który obejmie Radę, jej Sekretariat Generalny oraz państwa członkowskie.

(2) Przepisy niniejszej decyzji powinny mieć zastosowanie do przypadków, gdy Rada wykorzystuje do pracy informacje niejawne UE, jej organy przygotowawcze oraz Sekretariat Generalny Rady.

(3) Zgodnie z krajowymi przepisami ustawowymi i wykonawczymi i w zakresie, jaki jest niezbędny do funkcjonowania Rady, w przypadkach gdy właściwe organy, urzędnicy i wykonawcy państw członkowskich wykorzystują informacje niejawne UE podczas pracy, państwa członkowskie powinny przestrzegać przepisów niniejszej decyzji, tak aby każda ze stron mogła mieć pewność, że zagwarantowany

[1] Dz.U. L 285 z 16.10.2006, s. 47. Decyzja ostatnio zmieniona decyzją 2008/945/WE

został równoważny poziom ochrony informacji niejawnych UE.

(Dz.U. L 337 z 16.12.2008, s. 92).

(4) Rada i Komisja Europejska są zdecydowane stosować takie same normy bezpieczeństwa w celu ochrony informacji niejawnych UE.

(5) Rada podkreśla znaczenie włączania się, w odpowiednich przypadkach, Parlamentu Europejskiego i innych instytucji, agencji, organów lub biur UE w przestrzeganie zasad, norm i przepisów dotyczących ochrony informacji niejawnych, które są niezbędne do ochrony interesów Unii Europejskiej i państw członkowskich.

(6) Agencje i organy UE utworzone na mocy tytułu V lub VI Traktatu o Unii Europejskiej stosują w ramach swoich struktur wewnętrznych podstawowe zasady i minimalne normy określone w niniejszej decyzji w celu ochrony informacji niejawnych UE, zgodnie z tym, co przewidują akty założycielskie tych agencji i organów.

(7) Zasady bezpieczeństwa przyjęte przez Radę w celu ochrony informacji niejawnych UE stosuje się do operacji zarządzania kryzysowego organizowanych na mocy tytułu V Traktatu o Unii Europejskiej oraz do personelu biorącego w nich udział.

(8) Specjalni przedstawiciele UE i członkowie ich zespołów stosują zasady bezpieczeństwa przyjęte przez Radę w celu ochrony informacji niejawnych UE.

(9) Niniejsza decyzja zostaje przyjęta bez uszczerbku dla art. 255 i 286 Traktatu ustanawiającego Wspólnotę Europejską oraz aktów prawnych służących wykonaniu tych artykułów.

(10) Niniejsza decyzja zostaje przyjęta bez uszczerbku dla stosowanych w państwach członkowskich praktyk w zakresie powiadamiania parlamentów krajowych o działaniach UE,

STANOWI, CO NASTĘPUJE:

Artykuł 1

Cel, zakres zastosowania i definicje

1. Niniejsza decyzja określa podstawowe zasady i minimalne normy bezpieczeństwa służące ochronie informacji niejawnych UE.

2. Te podstawowe zasady i minimalne normy bezpieczeństwa mają zastosowanie do Rady i Sekretariatu Generalnego Rady (zwanego dalej „SGR"); państwa członkowskie muszą przestrzegać swoje krajowe przepisy ustawowe i wykonawcze, tak aby każda ze stron mogła mieć pewność, że zagwarantowany został równoważny poziom ochrony informacji niejawnych UE.

3. Do celów niniejszej decyzji zastosowanie mają definicje zamieszczone w dodatku A.

Artykuł 2

Definicja informacji niejawnych UE, klauzule tajności i oznaczenia dokumentu towarzyszące klauzuli

1. „Informacje niejawne UE" oznaczają wszelkie informacje lub materiały objęte klauzulą tajności UE, których nieuprawnione ujawnienie mogłoby w różnym stopniu wyrządzić szkodę interesom UE lub interesom co najmniej jednego państwa członkowskiego.

2. Informacjom niejawnym UE nadaje się jedną z następujących klauzul tajności[1]:

a) EU TOP SECRET TRES SECRET UE: informacje i materiały, których nieuprawnione ujawnienie mogłoby wyrządzić wyjątkowo poważną szkodę podstawowym interesom Unii Europejskiej lub co najmniej jednego państwa członkowskiego;

b) EU SECRET SECRET UE: informacje i materiały, których nieuprawnione ujawnienie mogłoby poważnie zaszkodzić podstawowym interesom Unii Europejskiej lub co najmniej jednego państwa członkowskiego;

c) EU CONFIDENTIAL CONFIDENTIEL UE: informacje i materiały, których nieuprawnione ujawnienie mogłoby zaszkodzić podstawowym interesom Unii Europejskiej lub co najmniej jednego państwa członkowskiego;

d) EU RESTRICTED RESTREINT UE: informacje i materiały, których nieuprawnione ujawnienie mogłoby być niekorzystne dla interesów Unii Europejskiej lub co najmniej jednego państwa członkowskiego.

3. Informacje niejawne UE opatrzone są oznaczeniem towarzyszącym klauzuli tajności zgodnie z ust. 2. Mogą być one opatrzone dodatkowym oznaczeniem wskazującym na dziedzinę działalności, do której się odnoszą, na wytwórcę, ograniczenia dystrybucji, na ograniczenia wykorzystania lub możliwość

---

[1] Dwadzieścia sześć delegacji opowiada się za stosowaniem oznaczeń towarzyszących klauzuli tylko w języku angielskim.
Co najmniej dwadzieścia trzy zaakceptowałyby także oznaczenia jednocześnie po angielsku I po francusku.
Jedna z delegacji opowiada się za utrzymaniem obecnej sytuacji (tzn. oznaczenia łączonego po francusku i angielsku towarzyszącego klauzuli TS-UE oraz po francusku w przypadku wszystkich innych klauzul); wariant ten może być zaakceptowany przez trzynaście delegacji.
W komitecie nie ma poparcia dla wyboru między oznaczeniami albo po angielsku, albo po francusku.
Większość delegacji uważa, że rozwiązanie należy znaleźć na szczeblu Komitetu ds. Bezpieczeństwa i że musi się ono opierać na względach bezpieczeństwa.
Komisja wyraża gotowość przychylenia się do ostatecznej opinii, jaką Komitet wyrazi w tej sprawie.
Uwaga: po osiągnięciu porozumienia w sprawie oznaczeń towarzyszących klauzulom tajności w całej decyzji wprowadzone zostaną odpowiednie zmiany.

ujawnienia.

Artykuł 3

Oznaczanie klauzulami

1. Właściwe organy dopilnowują, by informacjom niejawnym UE nadawano odpowiednie klauzule tajności, by informacje takie były wyraźnie oznaczone jako informacje niejawne, a także by były one objęte daną klauzulą nie dłużej, niż jest to konieczne.

2. Do obniżenia lub zniesienia klauzuli tajności nadanej informacjom niejawnym UE oraz do zmiany lub usunięcia oznaczeń, o których mowa w art. 2 ust. 3, potrzebna jest wcześniejsza pisemna zgoda wytwórcy.

3. Rada przyjmuje politykę bezpieczeństwa w zakresie tworzenia informacji niejawnych UE, która obejmuje praktyczny przewodnik nadawania klauzul.

Artykuł 4

Ochrona informacji niejawnych

1. Informacje niejawne UE są chronione zgodnie z przepisami niniejszej decyzji.

2. Posiadacz jakichkolwiek informacji niejawnych UE jest odpowiedzialny za ochronę ich zgodnie z przepisami niniejszej decyzji.

3. Jeżeli państwa członkowskie wprowadzają do struktur lub sieci UE informacje niejawne opatrzone krajowym oznaczeniem towarzyszącym klauzuli tajności, Rada i SGR obejmują te informacje ochroną zgodnie z wymogami, które mają zastosowanie do informacji niejawnych UE mających klauzulę o równoważnym poziomie – zgodnie z tabelą odpowiedników klauzul tajności zamieszczoną w dodatku B.

4. Uzasadnione może być objęcie dużych ilości lub zbioru informacji niejawnych UE ochroną na poziomie właściwym dla wyższej klauzuli.

Artykuł 5

Kontrola ryzyka naruszenia bezpieczeństwa

1. Kontrola ryzyka naruszenia informacji niejawnych UE przebiega w ramach określonego procesu. Proces ten jest ukierunkowany na określenie rodzajów ryzyka naruszenia bezpieczeństwa, środków bezpieczeństwa służących zmniejszeniu tego ryzyka do akceptowalnego poziomu zgodnie z podstawowymi zasadami i minimalnymi normami bezpieczeństwa przedstawionymi w niniejszej decyzji oraz na zastosowanie tych środków zgodnie z koncepcją głębokiej obrony. Skuteczność takich środków jest stale oceniana.

2. Środki bezpieczeństwa służące ochronie informacji niejawnych UE na wszystkich etapach ich istnienia są proporcjonalne w szczególności do ich klauzuli tajności, fizycznej postaci, ilości informacji lub materiałów, lokalizacji i konstrukcji obiektów, w których się znajdują, oraz oceny zagrożenia wystąpieniem w tym miejscu działań realizowanych w złych zamiarach lub działalności przestępczej, takiej jak działalność szpiegowska, sabotażowa lub terrorystyczna.

3. Plany awaryjne uwzględniają potrzebę ochrony informacji niejawnych UE podczas sytuacji nadzwyczajnych w celu zapobieżenia nieuprawnionemu dostępowi do informacji, ich ujawnieniu lub utracie ich integralności lub dostępności.

4. W planach ciągłości działania zamieszczane są środki zapobiegawcze i naprawcze służące zminimalizowaniu skutków poważnych niedopatrzeń lub incydentów związanych z pracą z wykorzystaniem informacji niejawnych UE oraz z ich przechowywaniem.

Artykuł 6

Wprowadzenie w życie przepisów niniejszej decyzji

1. Jeżeli to konieczne, Rada na zalecenie Komitetu ds. Bezpieczeństwa zatwierdza polityki bezpieczeństwa przewidujące środki, które służą wprowadzeniu w życie przepisów niniejszej decyzji.

2. Komitet ds. Bezpieczeństwa może na swoim poziomie uzgodnić wskazówki techniczne dotyczące bezpieczeństwa, które będą uzupełniać lub wspierać przepisy

niniejszej decyzji, oraz wszelkie polityki bezpieczeństwa zatwierdzone przez Radę.

Artykuł 7

Bezpieczeństwo osobowe

1. Bezpieczeństwo osobowe oznacza stosowanie środków, gwarantujących, że dostęp do informacji niejawnych UE będzie przyznawany tylko osobom, które:

   - podlegają zasadzie ograniczonego dostępu;

   - w stosownych przypadkach zostały sprawdzone pod względem bezpieczeństwa do celów dostępu do informacji o odnośnym poziomie; oraz

   - zostały poinformowane o swoich obowiązkach.

2. Procedury poświadczania bezpieczeństwa osobowego mają na celu stwierdzenie, czy daną osobę, ze względu na jej lojalność, wiarygodność i rzetelność, można uprawnić do dostępu do informacji niejawnych UE.

3. Wszystkie osoby pracujące w SGR, których obowiązki mogą wymagać dostępu do informacji niejawnych UE o klauzuli CONFIDENTIEL UE lub wyższej, są przed uzyskaniem dostępu do takich informacji sprawdzane pod względem bezpieczeństwa do odnośnego poziomu. Procedura poświadczania bezpieczeństwa osobowego urzędników i innych pracowników SGR przedstawiona jest w załączniku I.

4. Pracownicy państw członkowskich, o których mowa w art. 14 ust. 3 i których obowiązki mogą wymagać dostępu do informacji niejawnych UE o klauzuli CONFIDENTIEL UE lub wyższej, są przed uzyskaniem dostępu do takich informacji sprawdzani pod względem bezpieczeństwa do odnośnego poziomu lub otrzymują inne odpowiednie upoważnienie ze względu na pełnione przez siebie funkcje, zgodnie z krajowymi przepisami ustawowymi i wykonawczymi.

5. Przed uzyskaniem dostępu do informacji niejawnych UE, a następnie w regularnych odstępach czasu wszystkie osoby informowane są o obowiązku ochrony tych informacji zgodnie z niniejszą decyzją i potwierdzają znajomość tego obowiązku.

6. Przepisy dotyczące wprowadzania w życie niniejszego artykułu znajdują się w załączniku I.

Artykuł 8

Bezpieczeństwo fizyczne

1. Bezpieczeństwo fizyczne oznacza stosowanie środków ochrony fizycznej i technicznej, aby zapobiec nieuprawnionemu dostępowi do informacji niejawnych UE.

2. Środki bezpieczeństwa fizycznego mają na celu zapobiec wtargnięciu intruza, w sposób niezauważony lub z użyciem siły, powstrzymać od podjęcia nieuprawnionych działań, udaremniać i wykrywać oraz umożliwić podział pracowników pod względem dostępu do informacji niejawnych UE na podstawie zasady ograniczonego dostępu. Środki te określane są na podstawie procesu kontroli ryzyka.

3. Fizycznymi środkami bezpieczeństwa obejmuje się wszystkie obiekty, budynki, biura, pomieszczenia i inne strefy, w których są wykorzystywane do pracy lub przechowywane informacje niejawne UE, w tym strefy, w których znajdują się systemy łączności i informacji określone w art. 9.

4. W strefach, w których przechowywane są informacje niejawne UE o klauzuli tajności CONFIDENTIEL UE lub wyższej, tworzy się strefy zabezpieczone zgodnie z załącznikiem II; strefy takie zatwierdza właściwa władza bezpieczeństwa.

5. Do ochrony informacji niejawnych UE o klauzuli tajności CONFIDENTIEL UE lub wyższej stosuje się wyłącznie zatwierdzony sprzęt lub zatwierdzone urządzenia.

6. Przepisy dotyczące wprowadzania w życie niniejszego artykułu znajdują się w załączniku II.

Artykuł 9

Ochrona informacji niejawnych UE przetwarzanych w systemach łączności i informacji

1. Zabezpieczanie informacji w ramach systemów łączności i informacji oznacza pewność, że systemy te będą chronić informacje, które są przez nie wykorzystywane, i będą działać zgodnie z przeznaczeniem w razie potrzeby pod kontrolą uprawnionych użytkowników. Skuteczne zabezpieczanie informacji gwarantuje odpowiedni poziom poufności, integralności, dostępności, niezaprzeczalności i autentyczności. Zabezpieczanie informacji opiera się na procesie kontroli ryzyka.

2. System łączności i informacji oznacza system umożliwiający pracę z wykorzystaniem informacji w formie elektronicznej. System łączności i informacji obejmuje wszystkie zasoby niezbędne do jego funkcjonowania, w tym infrastrukturę, organizację, personel oraz zasoby informatyczne. Niniejsza decyzja ma zastosowanie do takich systemów przetwarzających informacje niejawne UE (zwanych dalej „CIS").

3. CIS przetwarza informacje niejawne UE zgodnie z koncepcją zabezpieczania informacji.

4. Wszystkie CIS poddawane są procedurze akredytacji. Celem akredytacji jest upewnienie się, że zastosowano wszystkie odpowiednie środki bezpieczeństwa i że osiągnięto wystarczający poziom ochrony informacji niejawnych UE i CIS – zgodnie z przepisami niniejszej decyzji. W poświadczeniu akredytacji określa się najwyższą klauzulę tajności informacji, które mogą być wykorzystywane do pracy w ramach danego CIS, oraz odnośne warunki.

5. CIS, w ramach których odbywa się praca z wykorzystaniem informacji o klauzuli CONFIDENTIEL UE i wyższej, są chronione w taki sposób, by bezpieczeństwo informacji nie mogło zostać narażone na szwank z powodu niezamierzonych emisji elektromagnetycznych („środki bezpieczeństwa TEMPEST").

6. Jeżeli informacje niejawne UE podlegają ochronie przy użyciu produktów kryptograficznych, produkty te są zatwierdzane w sposób następujący:

   a) Poufność informacji oznaczonych klauzulą SECRET UE i wyższą podlega ochronie przy użyciu produktów kryptograficznych zatwierdzonych – na podstawie zalecenia Komitetu ds. Bezpieczeństwa – przez Radę działającą jako organ ds. zatwierdzania produktów kryptograficznych (zwany dalej „CAA").

   b) Poufność informacji oznaczonych klauzulą CONFIDENTIEL UE lub RESTREINT UE podlega ochronie przy użyciu produktów kryptograficznych zatwierdzonych – na podstawie zalecenia Komitetu ds. Bezpieczeństwa – przez sekretarza generalnego Rady / wysokiego przedstawiciela ds. WPZiB (zwanego dalej „SG/WP") działającego jako CAA.

   Niezależnie od przepisów lit. b) w obrębie krajowych systemów państw członkowskich poufność informacji niejawnych UE oznaczonych klauzulą CONFIDENTIEL UE lub RESTREINT UE może być chroniona przy użyciu produktów kryptograficznych zatwierdzonych przez CAA danego państwa członkowskiego.

7. Podczas przekazywania informacji niejawnych UE drogą elektroniczną stosuje się zatwierdzone produkty kryptograficzne. Niezależnie od tego wymogu w wyjątkowych okolicznościach mogą mieć zastosowanie szczególne procedury lub szczególne konfiguracje techniczne określone w załączniku III.

8. Właściwe organy odpowiednio SGR i państw członkowskich ustanawiają następujące organy zajmujące się zabezpieczaniem informacji:

   a) organ ds. zabezpieczania informacji;

   b) organ ds. zatwierdzania produktów kryptograficznych (CAA);

c) organ ds. rozpowszechniania produktów kryptograficznych (CDA).

9. W odniesieniu do każdego systemu właściwe organy odpowiednio SGR i państw członkowskich ustanawiają:

   a) organ ds. akredytacji bezpieczeństwa (SAA);

   b) organ operacyjny ds. zabezpieczania informacji.

10. Przepisy dotyczące wprowadzania w życie niniejszego artykułu znajdują się w załączniku III.

Artykuł 10

Zarządzanie informacjami niejawnymi

1. Zarządzanie informacjami niejawnymi polega na stosowaniu środków administracyjnych służących kontroli informacji niejawnych UE na wszystkich etapach ich istnienia w uzupełnieniu środków przewidzianych w art. 7, 8 i 9, co ma pomóc powstrzymywać od zamierzonego lub przypadkowego narażenia na szwank bezpieczeństwa tych informacji lub ich utraty, wykrywać takie przypadki i usuwać ich skutki. Środki takie związane są w szczególności z wytwarzaniem, rejestracją, kopiowaniem, tłumaczeniem, przewożeniem i niszczeniem informacji niejawnych UE.

2. Informacje oznaczone klauzulą CONFIDENTIEL UE lub wyższą są ze względów bezpieczeństwa rejestrowane przed ich dystrybucją i w momencie wpłynięcia. Właściwe organy SGR i państw członkowskich ustanawiają do tego celu system kancelarii tajnych. Informacje oznaczone klauzulą TRES SECRET UE rejestruje się w wyznaczonych kancelariach tajnych.

3. Służby i obiekty, w których odbywa się praca z informacjami niejawnymi UE lub w których informacje te są przechowywane, są poddawane regularnym kontrolom przeprowadzanym przez właściwą władzę bezpieczeństwa.

4. Poza strefami chronionymi fizycznie informacje niejawne są przekazywane między służbami i obiektami w sposób następujący:

a) z reguły informacje niejawne UE są przekazywane drogą elektroniczną chronioną przy użyciu produktów kryptograficznych zatwierdzonych zgodnie z art. 9 ust. 6;

b) gdy ten sposób nie jest wykorzystywany, informacje niejawne UE są przekazywane:

(i) albo za pomocą środków elektronicznych (jak np. pamięć USB, płyty kompaktowe, twarde dyski) chronionych przy użyciu produktów kryptograficznych zatwierdzonych zgodnie z art. 9 ust. 6, tak by środek ten i jego zawartość (tj. kryptogram) mógł być przetwarzany i przechowywany jako materiał jawny;

(ii) albo, we wszystkich pozostałych przypadkach, zgodnie z wytycznymi właściwej władzy bezpieczeństwa wydanymi w myśl odnośnych środków ochrony określonych w załączniku IV.

5. Przepisy dotyczące wprowadzania w życie niniejszego artykułu znajdują się w załączniku IV.

Artykuł 11

Bezpieczeństwo przemysłowe

1. Bezpieczeństwo przemysłowe oznacza stosowanie środków mających zapewnić ochronę informacji niejawnych UE przez wykonawców lub podwykonawców podczas negocjacji poprzedzających zawarcie umów i na wszystkich etapach obowiązywania umów niejawnych. Umowy takie nie obejmują dostępu do informacji mających klauzulę TRES SECRET UE.

2. SGR może na podstawie umowy powierzyć zadania obejmujące informacje niejawne UE lub wiążące się z dostępem do tych informacji, ich wykorzystaniem do pracy lub przechowywaniem przez podmioty prowadzące działalność

przemysłową lub inną, zarejestrowane w państwie członkowskim lub w państwie trzecim, które zawarło z UE umowę o bezpieczeństwie informacji.

3. Jako instytucja zamawiająca, SGR dba o to, by w przypadku zawierania umów niejawnych z podmiotami prowadzącymi działalność przemysłową lub inną spełnione były minimalne normy bezpieczeństwa przemysłowego określone w niniejszej decyzji i te, o których mowa w danej umowie.

4. Krajowa władza bezpieczeństwa (zwana dalej „NSA"), wyznaczona władza bezpieczeństwa (zwana dalej „DSA") lub jakakolwiek inna właściwa władza bezpieczeństwa każdego państwa członkowskiego dbają o to, by – w zakresie, jaki umożliwiają to krajowe przepisy ustawowe i wykonawcze – wykonawcy i podwykonawcy zarejestrowani na ich terytorium stosowali wszelkie odpowiednie środki mające chronić informacje niejawne UE podczas negocjacji poprzedzających zawarcie umowy i podczas wykonywania umowy niejawnej.

5. NSA, DSA lub jakakolwiek inna właściwa władza bezpieczeństwa każdego państwa członkowskiego dbają o to, by zgodnie z krajowymi przepisami ustawowymi i wykonawczymi wykonawcy lub podwykonawcy zarejestrowani w tym państwie członkowskim będący stroną niejawnych umów o wykonawstwo lub podwykonawstwo i potrzebujący w swoich obiektach dostępu do informacji o klauzuli tajności CONFIDENTIEL UE lub SECRET UE podczas wykonywania takich umów lub na etapie poprzedzającym ich zawarcie posiadali świadectwo bezpieczeństwa przemysłowego (FSC) na odpowiednim poziomie klauzuli.

6. Odpowiednia NSA, DSA lub jakakolwiek inna właściwa władza bezpieczeństwa wydaje pracownikom wykonawcy lub podwykonawcy, których obowiązki związane z wykonaniem umowy niejawnej wymagają dostępu do informacji o klauzuli tajności CONFIDENTIEL UE lub SECRET UE, poświadczenie bezpieczeństwa osobowego (zwane dalej „PBO") – zgodnie z krajowymi przepisami ustawowymi i wykonawczymi oraz minimalnymi normami bezpieczeństwa określonymi w załączniku I do niniejszej decyzji.

7. Przepisy dotyczące wprowadzania w życie niniejszego artykułu znajdują się w załączniku V.

Artykuł 12

Wymiana informacji niejawnych z państwami trzecimi i organizacjami międzynarodowymi

1. Jeżeli Rada stwierdzi, że zachodzi konieczność wymiany informacji niejawnych UE z państwem trzecim lub organizacją międzynarodową, ustanowione zostają odpowiednie ramy takiej wymiany.

2. Aby ustanowić takie ramy i określić wzajemnie obowiązujące zasady ochrony wymienianych informacji niejawnych,

   a) Rada zawiera umowy dotyczące procedur bezpieczeństwa na potrzeby wymiany i ochrony informacji niejawnych (zwane dalej „umowami o bezpieczeństwie informacji"); lub

   b) SG/WP może zgodnie z pkt 17 załącznika VI zawierać porozumienia administracyjne, o ile poziom klauzuli nadanej informacjom niejawnym UE, które mają zostać udostępnione, nie jest z reguły wyższy niż RESTREINT UE.

3. Umowy o bezpieczeństwie informacji lub porozumienia administracyjne, o których mowa w ust. 2, obejmują postanowienia mające służyć temu, by w przypadku gdy państwa trzecie lub organizacje międzynarodowe otrzymują informacje niejawne UE, informacje te były chronione w sposób odpowiadający ich klauzuli i zgodny z minimalnymi normami, które nie mogą być mniej rygorystyczne niż normy określone w niniejszej decyzji.

4. Decyzja o udostępnieniu państwu trzeciemu lub organizacji międzynarodowej informacji niejawnych UE wytworzonych w Radzie podejmowana jest przez Radę po rozpatrzeniu każdego przypadku z osobna, w zależności od charakteru i treści takich informacji, od tego, czy odbiorca podlega zasadzie ograniczonego dostępu, i od tego, w jakim stopniu jest to korzystne dla UE. Jeżeli wytwórcą informacji niejawnych, o których udostępnienie wystąpiono, nie jest Rada, SGR najpierw zwraca się o pisemną zgodę wytwórcy na ich udostępnienie. Jeżeli nie można

ustalić, kto jest wytwórcą, Rada przejmuje jego odpowiedzialność.

5. Aby stwierdzić skuteczność środków bezpieczeństwa stosowanych w państwie trzecim lub organizacji międzynarodowej w celu ochrony informacji niejawnych UE, które zostały im przekazane jednostronnie lub w ramach wymiany, przeprowadzane są wizyty oceniające.

6. Przepisy dotyczące wprowadzania w życie niniejszego artykułu znajdują się w załączniku VI.

Artykuł 13

Naruszenie i narażenie na szwank bezpieczeństwa informacji niejawnych UE

1. Naruszenie bezpieczeństwa następuje w wyniku działania określonej osoby lub zaniechania przez nią działania w sposób sprzeczny z zasadami bezpieczeństwa ustanowionymi w niniejszej decyzji.

2. Narażenie na szwank bezpieczeństwa informacji niejawnych UE ma miejsce, gdy w wyniku naruszenia bezpieczeństwa takie informacje w całości lub w części zostają ujawnione osobom nieupoważnionym.

3. O wszelkich podejrzeniach lub przypadkach naruszenia bezpieczeństwa powiadamia się niezwłocznie właściwe władze bezpieczeństwa.

4. Jeżeli wiadomo lub istnieją uzasadnione powody, by przypuszczać, że bezpieczeństwo informacji niejawnych UE zostało narażone na szwank lub że informacje takie zostały utracone, właściwe władze bezpieczeństwa podejmują – zgodnie z odpowiednimi przepisami ustawowymi i wykonawczymi – wszelkie stosowne działania służące:

   - poinformowaniu o tym wytwórcy informacji;

   - zbadaniu tego przypadku przez personel niezwiązany bezpośrednio z tym naruszeniem w celu ustalenia przebiegu wydarzeń;

   - ocenie potencjalnych szkód dla interesów UE lub państw członkowskich;

   - podjęciu właściwych środków w celu zapobieżenia powtórzeniu się podobnego przypadku; oraz

- powiadomieniu właściwych organów o podjętych działaniach.

5. Każda osoba odpowiedzialna za naruszenie przepisów dotyczących bezpieczeństwa określonych w niniejszej decyzji może podlegać postępowaniu dyscyplinarnemu zgodnie z odpowiednimi przepisami ustawowymi i wykonawczymi. Każda osoba odpowiedzialna za narażenie na szwank bezpieczeństwa informacji niejawnych UE podlega postępowaniu dyscyplinarnemu lub sądowemu zgodnie z odpowiednimi przepisami ustawowymi, zasadami i przepisami wykonawczymi.

Artykuł 14

Odpowiedzialność za wdrożenie decyzji

1. Rada podejmuje wszelkie niezbędne działania w celu zapewnienia ogólnej spójności w stosowaniu niniejszej decyzji.

2. SG/WP podejmuje wszelkie niezbędne działania w celu zadbania o to, by przy pracy z wykorzystaniem informacji niejawnych UE lub jakichkolwiek innych informacji niejawnych lub przy przechowywaniu takich informacji w obiektach, z których korzysta Rada, oraz w obrębie SGR, w tym w obrębie biur łącznikowych znajdujących się w państwach trzecich, urzędnicy SGR i inni pracownicy, personel oddelegowany do SGR i wykonawcy zatrudnieni przez SGR przestrzegali przepisów niniejszej decyzji.

3. Państwa członkowskie podejmują – zgodnie ze swoimi przepisami ustawowymi i wykonawczymi – wszelkie stosowne działania w celu zadbania o to, by przy pracy z wykorzystaniem informacji niejawnych UE lub ich przechowywaniu przepisy niniejszej decyzji przestrzegali:

   a) pracownicy stałych przedstawicielstw państw członkowskich przy Unii Europejskiej, a także delegaci krajowi uczestniczący w posiedzeniach Rady lub jej organów przygotowawczych lub biorący udział w innych działaniach Rady;

   b) inni pracownicy administracji krajowej państw członkowskich, w tym pracownicy oddelegowani do pracy w administracji krajowej, gdy pełnią oni

obowiązki na terytorium państw członkowskich lub poza ich granicami;

c) inne osoby w państwach członkowskich, które ze względu na pełnione funkcje posiadają odpowiednie uprawnienia do dostępu do informacji niejawnych UE; oraz

d) wykonawcy zatrudnieni przez państwa członkowskie, na terytorium państw członkowskich lub poza ich granicami.

Artykuł 15

Organizacja bezpieczeństwa w Radzie

1. W ramach odpowiedzialności za zapewnianie ogólnej spójności w stosowaniu niniejszej decyzji Rada zatwierdza:

a) umowy, o których mowa w art. 12 ust. 2 lit. a);

b) decyzje w sprawie zezwolenia na udostępnienie informacji niejawnych UE państwom trzecim i organizacjom międzynarodowym;

c) roczny program kontroli proponowany przez SG/WP i zalecany przez Komitet ds. Bezpieczeństwa; program ten dotyczy kontroli służb i obiektów w państwach członkowskich i agencjach i organach UE oraz wizyt oceniających przeprowadzanych w państwach trzecich i w organizacjach międzynarodowych w celu sprawdzenia skuteczności środków wprowadzonych, by chronić informacje niejawne UE; oraz

d) polityki bezpieczeństwa przewidziane w art. 6 ust. 2.

2. Władzą bezpieczeństwa SGR jest SG/WP. Pełniąc tę funkcję, SG/WP:

a) wdraża politykę bezpieczeństwa opracowywaną przez Radę i dokonuje jej przeglądu;

b) koordynuje z NSA w państwach członkowskich wszystkie kwestie bezpieczeństwa związane z ochroną tych informacji niejawnych, które mają

związek z działaniami Rady;

c) wydaje PBO UE urzędnikom SGR i innym pracownikom zgodnie z art. 7 ust. 3, zanim będą mogli uzyskać dostęp do informacji o klauzuli CONFIDENTIEL UE lub wyższej;

d) w razie potrzeby zaleca zbadanie każdego zaistniałego lub domniemanego przypadku narażenia na szwank bezpieczeństwa informacji niejawnych znajdujących się w posiadaniu lub wytworzonych przez Radę lub utraty takich informacji oraz zwraca się do właściwych władz bezpieczeństwa o pomoc w takim badaniu;

e) przeprowadza okresowe kontrole zabezpieczeń służących ochronie informacji niejawnych w obiektach SGR;

f) przeprowadza okresowe kontrole zabezpieczeń służących ochronie informacji niejawnych UE w agencjach i organach UE, podczas operacji zarządzania kryzysowego prowadzonych na mocy tytułu V Traktatu o Unii Europejskiej oraz zabezpieczeń stosowanych przez specjalnych przedstawicieli UE i członków ich zespołów;

g) przeprowadza, wspólnie i w porozumieniu z zainteresowanymi NSA, okresowe kontrole zabezpieczeń służących ochronie informacji niejawnych UE w służbach i obiektach w państwach członkowskich;

h) koordynuje środki bezpieczeństwa z właściwymi organami państw członkowskich odpowiedzialnymi za ochronę informacji niejawnych oraz, w stosownych przypadkach, z państwami trzecimi lub organizacjami międzynarodowymi, w tym w zakresie charakteru zagrożeń dla bezpieczeństwa informacji niejawnych UE oraz środków ochrony przed tymi zagrożeniami;

i) zawiera porozumienia administracyjne, o których mowa w art. 12 ust. 2 lit. b); oraz

j) przeprowadza wstępne i okresowe wizyty oceniające w państwach trzecich lub w organizacjach międzynarodowych w celu sprawdzenia skuteczności środków wprowadzonych, by chronić informacje niejawne UE przekazane im jednostronnie lub w ramach wymiany.

Biuro ds. Bezpieczeństwa SGR pozostaje do dyspozycji SG/WP i pomaga mu w wypełnianiu wyżej opisanych obowiązków.

3. W celu wprowadzenia w życie art. 14 ust. 3 państwa członkowskie:

a) wyznaczają NSA odpowiedzialne za zabezpieczenia służące ochronie informacji niejawnych UE. NSA wymienione są w dodatku C. W każdym państwie członkowskim NSA wprowadzają wszelkie odpowiednie środki zapewniające:

(i) ochronę, zgodnie z przepisami niniejszej decyzji, informacji niejawnych UE znajdujących się w posiadaniu jakiegokolwiek podmiotu krajowego: departamentu, organu lub agencji, bez względu na to, czy jest to podmiot publiczny czy prywatny i czy znajduje się w kraju czy za granicą;

(ii) okresowe kontrole zabezpieczeń służących ochronie informacji niejawnych UE;

(iii) odpowiednie sprawdzenie pod względem bezpieczeństwa wszystkich osób, które są zatrudnione w administracji krajowej lub przez wykonawcę i które mogą uzyskać dostęp do informacji UE o klauzuli CONFIDENTIEL UE lub wyższej, lub przyznanie tym osobom ze względu na pełnione przez nie funkcje innych właściwych uprawnień zgodnie z krajowymi przepisami ustawowymi i wykonawczymi;

(iv) opracowanie takich programów bezpieczeństwa, które są potrzebne, aby bezpieczeństwo informacji niejawnych UE nie zostało narażone na szwank lub informacje takie nie zostały utracone; oraz

(v) koordynację z innymi właściwymi organami krajowymi, w tym z organami, o których mowa w niniejszej decyzji, kwestii bezpieczeństwa związanych z ochroną informacji niejawnych UE;

b) dopilnowują, by ich właściwe organy dostarczały informacje i doradzały rządowi, a za jego pośrednictwem Radzie co do charakteru zagrożeń dla bezpieczeństwa informacji niejawnych UE i środków ochrony przed tymi zagrożeniami; oraz

c) rozpatrują wnioski o wydanie poświadczenia bezpieczeństwa składane przez agencje i organy UE, w ramach operacji zarządzania kryzysowego ustanowionych na mocy tytułu V Traktatu o Unii Europejskiej oraz przez specjalnych przedstawicieli UE (SPUE) i ich zespoły.

Artykuł 16

Komitet ds. Bezpieczeństwa

1. Niniejszym ustanawia się Komitet ds. Bezpieczeństwa. Komitet analizuje i ocenia wszelkie kwestie bezpieczeństwa, które wchodzą w zakres zastosowania niniejszej decyzji, oraz przedstawia Radzie odpowiednie zalecenia.

2. Komitet ds. Bezpieczeństwa składa się z przedstawicieli NSA państw członkowskich, a w jego obradach uczestniczy przedstawiciel Komisji Europejskiej. Przewodniczy mu SG/WP lub wyznaczona przez niego osoba. Komitet ten zbiera się na polecenie Rady lub na wniosek SG/WP lub NSA.

   Do uczestnictwa w pracach Komitetu mogą zostać zaproszeni przedstawiciele agencji i organów UE, jeżeli omawiane są kwestie, które ich dotyczą.

3. Komitet ds. Bezpieczeństwa organizuje swoją działalność w taki sposób, aby móc przedstawiać zalecenia w konkretnych dziedzinach dotyczących bezpieczeństwa. Ustala on poddziedzinę pracy ekspertów zajmujących się kwestiami zabezpieczenia informacji oraz inne poddziedziny pracy ekspertów, zależnie od konieczności. Wyznacza on zakres zadań ekspertów w ramach takich poddziedzin i otrzymuje od nich sprawozdania z działalności, w tym – w zależności od sytuacji – zalecenia dla Rady.

Artykuł 17

Zastąpienie poprzednich decyzji

1. Niniejsza decyzja uchyla i zastępuje decyzję Rady 2001/264/WE[1] w sprawie przyjęcia przepisów Rady dotyczących bezpieczeństwa oraz wszelkie późniejsze zmiany tej decyzji.

2. Wszystkie informacje niejawne UE opatrzone klauzulą zgodnie z decyzją Rady 2001/264/WE podlegają dalszej ochronie zgodnie z odnośnymi przepisami niniejszej

[1] Dz.U. L 101 z 11.4.2001, s. 1.

decyzji.

Artykuł 18

Wejście w życie

Niniejszą decyzję stosuje się od daty jej opublikowania.

Sporządzono w Brukseli, xx

W imieniu Rady

Przewodniczący

ZAŁĄCZNIKI

ZAŁĄCZNIK I

Bezpieczeństwo osobowe

ZAŁĄCZNIK II

Bezpieczeństwo fizyczne

ZAŁĄCZNIK III

Ochrona informacji niejawnych UE przetwarzanych w systemach łączności i informacji

ZAŁĄCZNIK IV

Zarządzanie informacjami niejawnymi

ZAŁĄCZNIK V

Bezpieczeństwo przemysłowe

ZAŁĄCZNIK VI

Wymiana informacji niejawnych z państwami trzecimi i organizacjami międzynarodowymi

ZAŁĄCZNIK I

BEZPIECZEŃSTWO OSOBOWE

I. WPROWADZENIE

1. Niniejszy załącznik zawiera przepisy dotyczące wprowadzania w życie art. 7. W niniejszym załączniku określa się w szczególności kryteria wykorzystywane do oceny, czy określoną osobę ze względu na jej lojalność, wiarygodność i rzetelność można uprawnić do dostępu do informacji niejawnych UE, a także procedury sprawdzające i administracyjne, które należy stosować w tym celu.

2. W całym niniejszym załączniku, z wyjątkiem miejsc, w których rozróżnienie to jest istotne, termin „poświadczenie bezpieczeństwa osobowego" odnosi się do krajowego poświadczenia bezpieczeństwa osobowego („krajowego PBO") lub do poświadczenia bezpieczeństwa osobowego UE („PBO UE") zdefiniowanych w dodatku A.

II. PRZYZNAWANIE UPRAWNIEŃ DO DOSTĘPU DO INFORMACJI NIEJAWNYCH UE

3. Daną osobę można uprawnić do dostępu do informacji o klauzuli CONFIDENTIEL UE lub wyższej wyłącznie po tym, jak:

   (a) stwierdzono, że podlega ona zasadzie ograniczonego dostępu; oraz

   (b) przyznano jej PBO do odnośnego poziomu lub ze względu na pełnione przez nią funkcje przyznano jej inne odpowiednie uprawnienia zgodnie z krajowymi przepisami ustawowymi i wykonawczymi; oraz

(c) została ona poinformowana o zasadach i procedurach bezpieczeństwa służących ochronie informacji niejawnych UE i potwierdziła, że zapoznała się ze swoimi obowiązkami w zakresie ochrony takich informacji.

4. Każde państwo członkowskie i SGR określają, które stanowiska w ich strukturach wymagają dostępu do informacji o klauzuli CONFIDENTIEL UE lub wyższej, i w związku z tym wymagają PBO do odnośnego poziomu.

III. WYMOGI DOTYCZĄCE POŚWIADCZENIA BEZPIECZEŃSTWA OSOBOWEGO

5. Po otrzymaniu wniosku z odpowiedniego upoważnienia NSA lub inne właściwe organy krajowe są odpowiedzialne za dopilnowanie, by przeprowadzono postępowanie sprawdzające w zakresie bezpieczeństwa w odniesieniu do obywateli ich kraju, którym potrzebny jest dostęp do informacji o klauzuli CONFIDENTIEL UE lub wyższej. Normy postępowania sprawdzającego są zgodne z krajowymi przepisami ustawowymi i wykonawczymi.

6. Jeżeli miejsce pobytu danej osoby znajduje się na terytorium innego państwa członkowskiego lub państwa trzeciego, właściwe organy krajowe zwracają się o pomoc do właściwego organu państwa pobytu zgodnie z krajowymi przepisami ustawowymi i wykonawczymi. Państwa członkowskie wzajemnie się wspierają w prowadzeniu postępowań sprawdzających w zakresie bezpieczeństwa zgodnie z krajowymi przepisami ustawowymi i wykonawczymi.

7. Jeżeli krajowe przepisy ustawowe i wykonawcze dopuszczają taką możliwość, krajowe władze bezpieczeństwa lub inne właściwe organy krajowe mogą przeprowadzać postępowania sprawdzające w odniesieniu do osób niebędących obywatelami ich kraju, którym potrzebny jest dostęp do informacji o klauzuli CONFIDENTIEL UE lub wyższej. Normy postępowania sprawdzającego są zgodne z krajowymi przepisami ustawowymi i wykonawczymi.

Kryteria postępowania sprawdzającego

8. W celu wydania danej osobie PBO upoważniającego ją do dostępu do informacji o klauzuli CONFIDENTIEL UE lub wyższej sprawdza się jej lojalność, wiarygodność i rzetelność za pomocą postępowania sprawdzającego. Na podstawie wyników takiego postępowania właściwy organ krajowy dokonuje ogólnej oceny. Pojedyncza niekorzystna informacja uzyskana w wyniku postępowania nie musi skutkować odmową wydania PBO. Główne kryteria stosowane powinny w tym celu obejmować – w zakresie, jaki umożliwiają to krajowe przepisy ustawowe i wykonawcze – ustalenie, czy osoba ta:

(a) popełniła lub usiłowała popełnić akt szpiegostwa, terroryzmu, sabotażu, zdrady lub podżegania, współpracowała z inną osobą w celu popełnienia takiego aktu, pomagała innej osobie w jego popełnieniu lub nakłaniała inne osoby do popełnienia takiego aktu;

(b) współdziała lub współdziałała ze szpiegami, terrorystami, sabotażystami lub osobami, co do których istnieje uzasadnione podejrzenie, że nimi są, lub z przedstawicielami organizacji obcych państw, w tym obcych służb wywiadowczych, które mogą stanowić zagrożenie dla bezpieczeństwa UE lub państw członkowskich, chyba że udzielono zezwolenia na takie współdziałanie w ramach obowiązków służbowych;

(c) jest lub była członkiem organizacji, która za pomocą aktów przemocy, działalności wywrotowej lub innych nielegalnych środków dąży do obalenia rządu jednego z państw członkowskich lub zmiany formy rządów w jednym z państw członkowskich;

(d) jest lub była stronnikiem jakiejkolwiek organizacji opisanej w lit. c) lub blisko współdziała lub blisko współdziałała z członkami takich organizacji;

(e) świadomie zataiła, przeinaczyła lub sfałszowała istotne informacje, szczególnie informacje związane z bezpieczeństwem, lub świadomie skłamała przy wypełnianiu ankiety bezpieczeństwa osobowego lub podczas rozmowy dotyczącej bezpieczeństwa osobowego;

(f) została skazana za popełnienie jednego przestępstwa lub większej ich liczby;

(g) kiedykolwiek była uzależniona od alkoholu, zażywała nielegalne środki odurzające lub nadużywała legalnych środków odurzających;

(h) zachowuje się lub zachowywała w sposób powodujący ryzyko podatności na szantaż lub presję;

(i) w czynach lub słowach wykazała się nieuczciwością, nielojalnością, brakiem rzetelności lub wiarygodności;

(j) poważnie lub wielokrotnie naruszyła przepisy dotyczące bezpieczeństwa lub usiłowała dokonać albo dokonała czynności, do których nie była uprawniona, w odniesieniu do systemów łączności i informacji;

(k) może podlegać presji krewnych lub bliskich współpracowników, którzy mogą być podatni na wpływy obcych służb wywiadowczych, grup terrorystycznych lub innych wywrotowych organizacji lub osób w celach mogących zagrażać interesom bezpieczeństwa UE lub państw członkowskich.

9. W stosownych przypadkach oraz zgodnie z krajowymi przepisami ustawowymi i wykonawczymi podczas postępowania sprawdzającego w zakresie bezpieczeństwa za istotną można uznać także sytuację finansową i zdrowotną danej osoby.

10. Posiadanie podwójnego obywatelstwa, z których jedno nie jest obywatelstwem UE, nie stanowi samo w sobie podstawy do odmowy wydania PBO.

11. W stosownych przypadkach oraz zgodnie z krajowymi przepisami ustawowymi i wykonawczymi podczas postępowania sprawdzającego w zakresie bezpieczeństwa za istotne można uznać także charakter, zachowanie i sytuację współmałżonka danej osoby, jej partnera życiowego lub członka bliskiej rodziny.

Wymogi postępowania sprawdzającego na potrzeby dostępu do informacji niejawnych UE

Przyznanie pierwszego PBO

12. Pierwsze PBO upoważniające do dostępu do informacji o klauzulach CONFIDENTIEL UE i SECRET UE wydawane jest po przeprowadzeniu postępowania sprawdzającego obejmującego co najmniej okres ostatnich pięciu lat lub okres od ukończenia 18. roku życia do chwili obecnej, w zależności od tego, który z tych okresów jest krótszy; postępowanie obejmuje:

(a) wypełnienie krajowej ankiety bezpieczeństwa osobowego na poziomie odpowiadającym klauzuli nadanej informacjom niejawnym UE, do których dostęp może być potrzebny danej osobie; wypełniona ankieta przekazywana jest właściwej władzy bezpieczeństwa;

(b) sprawdzenie tożsamości / obywatelstwa / narodowości – potwierdza się datę i miejsce urodzenia danej osoby i sprawdza się jej tożsamość. Ustala się przeszłe i obecne obywatelstwo lub narodowość danej osoby; obejmuje to ocenę podatności na presję osób z zagranicy, na przykład w związku z poprzednim miejscem pobytu lub przeszłymi powiązaniami; oraz

(c) sprawdzenie rejestrów krajowych i lokalnych – sprawdzane są krajowe rejestry bezpieczeństwa i centralne rejestry karne, o ile te ostatnie istnieją, lub inne porównywalne rejestry rządowe i policyjne. Sprawdza się rejestry organów ścigania sprawujących jurysdykcję w miejscach, w których dana osoba miała miejsce pobytu lub była zatrudniona.

13. Pierwsze PBO upoważniające do dostępu do informacji o klauzuli TRES SECRET UE wydawane jest po przeprowadzeniu postępowania sprawdzającego obejmującego co najmniej okres ostatnich dziesięciu lat lub okres od ukończenia 18. roku życia do chwili obecnej, w zależności od tego, który z tych okresów jest krótszy. Jeżeli zgodnie z poniższym ppkt e) przeprowadzane są rozmowy, postępowanie sprawdzające obejmuje okres co najmniej ostatnich siedmiu lat lub okres od ukończenia 18. roku życia do chwili obecnej, w zależności od tego, który okres jest krótszy. Poza kryteriami określonymi w pkt 8 przed wydaniem PBO na poziomie TRES SECRET UE należy zbadać elementy wymienione poniżej; elementy te można również zbadać przed wydaniem PBO na poziomie CONFIDENTIEL UE lub SECRET UE, jeżeli wymagają tego krajowe przepisy ustawowe i wykonawcze:

(a) status finansowy – poszukuje się informacji dotyczących sytuacji finansowej danej osoby, aby ocenić stopień podatności na presję osób z kraju lub z zagranicy z powodu poważnych trudności finansowych lub aby ujawnić wszelkie przychody z nieznanych źródeł;

(b) wykształcenie – poszukuje się informacji na temat szkół, szkół wyższych lub innych placówek edukacyjnych, do których uczęszczała dana osoba od ukończenia 18. roku życia lub w okresie, który organ prowadzący postępowanie sprawdzające uzna za odpowiedni;

(c) zatrudnienie – poszukuje się informacji dotyczących obecnego i poprzedniego zatrudnienia, przy wykorzystaniu takich źródeł jak historia zatrudnienia, sprawozdania dotyczące wyników lub wydajności pracy oraz opinie pracodawców lub przełożonych;

(d) służba wojskowa – w stosownych przypadkach weryfikowany jest stosunek danej osoby do służby wojskowej oraz powód zwolnienia ze służby; oraz

(e) rozmowy – pod warunkiem że przepisy krajowe przewidują i dopuszczają taką możliwość, przeprowadza się z daną osobą co najmniej jedną rozmowę. Rozmowy przeprowadza się również z innymi osobami, które są w stanie przedstawić obiektywną ocenę dotyczącą pochodzenia, działalności, lojalności, wiarygodności i rzetelności osoby sprawdzanej. W przypadku gdy krajowa praktyka przewiduje przedstawianie referencji przez osobę sprawdzaną, przeprowadza się rozmowę z osobami, które dostarczyły tych referencji, chyba że istnieją uzasadnione powody, żeby tego nie czynić.

14. Jeżeli jest to konieczne i zgodne z krajowymi przepisami ustawowymi i wykonawczymi, można przeprowadzić dodatkowe postępowania sprawdzające w celu rozwinięcia wszelkich dostępnych istotnych informacji dotyczących danej osoby oraz w celu potwierdzenia lub wykazania fałszywości informacji działających na niekorzyść osoby sprawdzanej.

Przedłużanie ważności PBO

15. Po przyznaniu pierwszego PBO oraz pod warunkiem że w zatrudnieniu danej osoby w administracji krajowej lub w SGR nie występują przerwy, a dostęp do informacji niejawnych UE jest jej stale potrzebny, przedłużenie ważności PBO tej osoby rozpatrywane jest w odstępach czasu nieprzekraczających 5 lat w przypadku poświadczenia dotyczącego klauzuli TRES SECRET UE oraz 10 lat w przypadku poświadczeń upoważniających do dostępu do klauzul SECRET UE i CONFIDENTIEL UE, licząc od daty powiadomienia o wyniku ostatniego postępowania sprawdzającego w zakresie bezpieczeństwa, na podstawie którego zostały wydane te poświadczenia. Wszelkie postępowania sprawdzające w zakresie bezpieczeństwa dotyczące przedłużenia PBO obejmują okres od poprzedniego postępowania.

16. W celu przedłużenia ważności PBO należy zbadać elementy przedstawione w pkt 12 i 13.

17. Wnioski o przedłużenie ważności składane są z odpowiednim wyprzedzeniem, z uwzględnieniem czasu potrzebnego do przeprowadzenia postępowań sprawdzających w zakresie bezpieczeństwa. Jeżeli jednak odpowiednie NSA lub inne właściwe organy krajowe otrzymały dany wniosek o przedłużenie ważności oraz odnośną ankietę bezpieczeństwa osobowego, zanim PBO utraciło ważność, a niezbędne postępowanie sprawdzające w zakresie bezpieczeństwa nie zostało jeszcze zakończone, właściwy organ krajowy może przedłużyć ważność obowiązującego PBO o okres nieprzekraczający 12 miesięcy, jeżeli dopuszczają to krajowe przepisy ustawowe i wykonawcze. Jeżeli na koniec tego dwunastomiesięcznego okresu nadal nie zakończono postępowania sprawdzającego w zakresie bezpieczeństwa, danej osobie przyznaje się obowiązki, które nie wymagają posiadania PBO.

Procedury związane z wydaniem PBO obowiązujące w SGR

18. W przypadku urzędników i innych pracowników SGR władze bezpieczeństwa SGR przekazują wypełnioną ankietę bezpieczeństwa osobowego NSA działającym w państwie członkowskim, którego obywatelem jest dana osoba, z prośbą o przeprowadzenie postępowania sprawdzającego w zakresie bezpieczeństwa dotyczącego takiego poziomu informacji niejawnych UE, do jakiego będzie potrzebować dostępu dana osoba.

19. Jeżeli SGR znajdzie się w posiadaniu informacji dotyczącej osoby, która złożyła wniosek o PBO UE, i istotnej w odniesieniu do postępowania sprawdzającego w zakresie bezpieczeństwa, powiadamia o tym odnośne NSA, działając zgodnie z odnośnymi zasadami i przepisami wykonawczymi.

20. Po zakończeniu postępowania sprawdzającego w zakresie bezpieczeństwa odpowiednie NSA powiadamiają władze bezpieczeństwa SGR, w formacie korespondencji określonym przez Komitet ds. Bezpieczeństwa, o wyniku takiego postępowania.

    a) Jeżeli w wyniku postępowania sprawdzającego uzyskuje się pewność, że nie istnieją żadne niekorzystne okoliczności, które mogłyby podważać lojalność, wiarygodność i rzetelność danej osoby, organ powołujący SGR może wydać tej osobie PBO UE oraz upoważnić ją do dostępu do informacji niejawnych UE do odpowiedniego poziomu i do określonej daty.

    b) Jeżeli postępowanie sprawdzające nie daje takiej pewności, organ powołujący SGR powiadamia o tym fakcie daną osobę, a ona może się do niego zwrócić z prośbą o wysłuchanie. Organ powołujący może zwrócić się do właściwych NSA o przedstawienie wszelkich dalszych wyjaśnień, jakich władze te mogą dostarczyć zgodnie z krajowymi przepisami ustawowymi i wykonawczymi. Jeżeli wynik zostanie potwierdzony, nie wydaje się PBO UE.

21. Postępowanie sprawdzające w zakresie bezpieczeństwa oraz jego wyniki podlegają odnośnym przepisom ustawowym i wykonawczym obowiązującym w danym państwie członkowskim, w tym także środkom odwoławczym. Decyzje organu powołującego SGR podlegają środkom odwoławczym zgodnie z Regulaminem pracowniczym urzędników Wspólnot Europejskich i warunkami zatrudnienia innych pracowników Wspólnot Europejskich.

22. Pewność, która stanowi podstawę PBO UE, o ile nadal istnieje, odnosi się do każdego zadania powierzonego danej osobie w SGR lub Komisji Europejskiej.

23. Jeżeli okres wykonywania przez daną osobę obowiązków służbowych nie rozpocznie się w terminie 12 miesięcy od powiadomienia organu powołującego SGR o wyniku postępowania sprawdzającego w zakresie bezpieczeństwa lub jeżeli w pełnieniu obowiązków przez daną osobę występuje dwunastomiesięczna przerwa, w czasie której osoba ta nie jest zatrudniona w SGR ani na żadnym stanowisku w administracji krajowej państwa członkowskiego, wynik postępowania sprawdzającego jest przekazywany odpowiednim NSA w celu upewnienia się, że jest nadal ważny i właściwy.

24. Jeżeli SGR znajdzie się w posiadaniu informacji o ryzyku naruszenia bezpieczeństwa przez osobę, która posiada ważne PBO UE, powiadamia o tym odnośne NSA, działając zgodnie z odnośnymi zasadami i przepisami wykonawczymi. Jeżeli NSA powiadomią SGR o utracie pewności uzyskanej zgodnie z pkt 20 ppkt a) w odniesieniu do osoby posiadającej ważne PBO UE, organ powołujący SGR może zwrócić się do NSA o przedstawienie wszelkich dalszych wyjaśnień, jakich władze te mogą dostarczyć zgodnie z krajowymi przepisami ustawowymi i wykonawczymi. Jeżeli niekorzystne informacje zostaną potwierdzone, PBO UE zostaje wycofane, a osobie takiej odbiera się prawo dostępu do informacji niejawnych UE i odsuwa się ją od stanowisk, na których taki dostęp jest możliwy lub na których osoba ta mogłaby zagrażać bezpieczeństwu.

25. O każdej decyzji w sprawie wycofania PBO UE przyznanego urzędnikowi lub innemu pracownikowi SGR i, w odpowiednich przypadkach, o przyczynach tego wycofania powiadamia się daną osobę, a ona może zwrócić się do organu powołującego z prośbą o wysłuchanie. Informacje przedstawione przez NSA podlegają odnośnym przepisom ustawowym i wykonawczym obowiązującym w danym państwie członkowskim, w tym także środkom odwoławczym. Decyzje organu powołującego SGR podlegają środkom odwoławczym zgodnie z Regulaminem pracowniczym urzędników Wspólnot Europejskich i warunkami zatrudnienia innych pracowników Wspólnot Europejskich.

26. Eksperci krajowi oddelegowani do SGR na stanowisko wymagające PBO UE są zobowiązani do przedstawienia władzy bezpieczeństwa SGR – przed rozpoczęciem wykonywania swoich zadań – ważnego krajowego PBO.

Akta dotyczące PBO

27. Akta dotyczące krajowych PBO i PBO UE wydanych w celu umożliwienia dostępu do informacji niejawnych UE są przechowywane, odpowiednio, przez każde państwo członkowskie i przez SGR. Akta te zawierają co najmniej informacje o klauzuli tajności nadanej informacjom niejawnym UE, do których dana osoba może mieć dostęp (CONFIDENTIEL UE lub wyższy), dacie wydania PBO i okresie jego ważności.

28. Właściwa władza bezpieczeństwa może wydać certyfikat potwierdzający posiadanie poświadczenia bezpieczeństwa osobowego zawierający informacje o klauzuli tajności nadanej informacjom niejawnym UE, do których dana osoba może mieć dostęp (CONFIDENTIEL UE lub wyższy), okresie ważności odnośnego krajowego PBO lub PBO UE oraz dacie ważności samego certyfikatu.

Zwolnienia z wymogu posiadania PBO

29. Dostęp osób odpowiednio uprawnionych ze względu na pełnione przez nie funkcje w państwach członkowskich do informacji niejawnych UE określany jest zgodnie z krajowymi przepisami ustawowymi i wykonawczymi; osoby takie są informowane o spoczywających na nich obowiązkach dotyczących bezpieczeństwa w zakresie ochrony informacji niejawnych UE.

IV. SZKOLENIA I UPOWSZECHNIANIE WIEDZY W DZIEDZINIE BEZPIECZEŃSTWA

30. Wszystkie osoby, którym przyznano PBO, potwierdzają na piśmie, że zrozumiały spoczywające na nich obowiązki w zakresie ochrony informacji niejawnych UE i konsekwencje narażenia na szwank bezpieczeństwa tych informacji. Dokumentacja dotycząca takiego pisemnego potwierdzenia przechowywana jest, odpowiednio, przez państwo członkowskie i przez SGR.

31. Wszystkie osoby, które są upoważnione do dostępu do informacji niejawnych UE lub muszą korzystać z tych informacji podczas pracy, na początku powiadamiane są o zagrożeniach bezpieczeństwa, a następnie regularnie przypomina się im o tych zagrożeniach; osoby te muszą bezzwłocznie zgłaszać właściwym władzom bezpieczeństwa wszelkie zdarzenia lub wszelką działalność, które uznają za podejrzane lub nietypowe.

32. Wszystkie osoby, które przestają wykonywać obowiązki wymagające dostępu do informacji niejawnych UE, powiadamiane są o obowiązku stałej ochrony tych informacji; w odpowiednich przypadkach świadomość tego obowiązku potwierdzają one na piśmie.

V. OKOLICZNOŚCI WYJĄTKOWE

33. Jeżeli krajowe przepisy ustawowe i wykonawcze dopuszczają taką możliwość, poświadczenie bezpieczeństwa osobowego przyznane przez właściwy organ krajowy państwa członkowskiego i uprawniające do dostępu do krajowych informacji niejawnych może, podczas oczekiwania na wydanie krajowego PBO uprawniającego do dostępu do informacji niejawnych UE, tymczasowo uprawniać urzędników krajowych do dostępu do informacji niejawnych UE do poziomu równoważnego poziomowi określonemu w tabeli odpowiedników klauzul tajności, którą zamieszczono w dodatku B, o ile takiego tymczasowego dostępu wymaga interes UE. Jeżeli krajowe przepisy ustawowe i wykonawcze nie zezwalają na taki tymczasowy dostęp do informacji niejawnych UE, NSA informują o tym Komitet ds. Bezpieczeństwa.

34. W sytuacjach wymagających szybkiego działania, jeżeli jest to uzasadnione interesami służby, w oczekiwaniu na zakończenie pełnego postępowania sprawdzającego organ powołujący SGR może, po konsultacji z NSA państwa członkowskiego, którego obywatelem jest dana osoba, oraz z zastrzeżeniem, że kontrole wstępne nie wykazały niekorzystnych informacji, wydać urzędnikom i innym pracownikom SGR tymczasowe upoważnienie do dostępu do informacji niejawnych UE, by mogli wykonać określone zadania. Takie tymczasowe upoważnienia zachowują ważność przez okres nieprzekraczający sześciu miesięcy i nie uprawniają do dostępu do informacji o klauzuli TRES SECRET UE. Wszystkie osoby, którym przyznano tymczasowe upoważnienie, potwierdzają na piśmie, że zrozumiały spoczywające na nich obowiązki w zakresie ochrony informacji niejawnych UE i konsekwencje narażenia na szwank bezpieczeństwa tych informacji. Dokumentacja dotycząca takiego pisemnego potwierdzenia przechowywana jest przez SGR.

35. Jeżeli dana osoba ma objąć stanowisko, które wymaga PBO na poziomie wyższym od posiadanego przez nią w danym momencie, może ona tymczasowo pełnić obowiązki związane z tym stanowiskiem, pod warunkiem że:

    (a) bezwzględna potrzeba dostępu do informacji niejawnych UE o wyższej klauzuli jest uzasadniona na piśmie przez przełożonego tej osoby;

(b) dostęp jest ograniczony do konkretnych informacji niejawnych UE, które są potrzebne do pracy na tym stanowisku;

(c) osoba ta posiada ważne krajowe PBO lub PBO UE;

(d) podjęto czynności w celu uzyskania upoważnienia do dostępu do informacji na poziomie wymaganym na tym stanowisku;

(e) właściwy organ przeprowadził kontrole, które potwierdziły, że dana osoba nie naruszała poważnie ani wielokrotnie przepisów dotyczących bezpieczeństwa;

(f) objęcie tego stanowiska przez daną osobę zatwierdził właściwy organ; oraz

(g) dokumentacja tego wyjątkowego przyznania dostępu, wraz z opisem informacji, do których zatwierdzono dostęp, przechowywana jest w odpowiedzialnej kancelarii tajnej lub podległej kancelarii tajnej.

36. Powyższa procedura jest stosowana, by przyznać danej osobie jednorazowy dostęp do informacji niejawnych UE o klauzuli o jeden stopień wyższej niż klauzula, do której ma ona dostęp na podstawie sprawdzenia pod względem bezpieczeństwa. Z procedury tej nie korzysta się w sposób powtarzający się.

37. W wyjątkowych okolicznościach, tj. w przypadku misji prowadzonych we wrogim środowisku lub w okresie rosnącego napięcia międzynarodowego, i gdy wymagają tego środki nadzwyczajne, w szczególności ratowanie życia ludzkiego, państwa członkowskie i SG/WP lub zastępca Sekretarza Generalnego mogą udzielić, w miarę możliwości na piśmie, dostępu do informacji niejawnych o klauzuli CONFIDENTIEL UE lub SECRET UE osobom, które nie posiadają wymaganego PBO, pod warunkiem że takie zezwolenie jest absolutnie niezbędne i nie ma żadnych uzasadnionych wątpliwości co do lojalności, wiarygodności i rzetelności danej osoby. Zachowuje się dokumentację takiego zezwolenia zawierającą opis informacji, do których dostęp zatwierdzono.

38. Dostęp do informacji oznaczonych klauzulą TRES SECRET UE w sytuacjach nadzwyczajnych przysługuje tylko obywatelom UE, których upoważniono do dostępu do krajowego odpowiednika klauzuli TRES SECRET UE lub do informacji oznaczonych klauzulą SECRET UE.

39. Komitet ds. Bezpieczeństwa informowany jest o przypadkach skorzystania z procedury przedstawionej w pkt 37 i 38.

40. Jeżeli krajowe przepisy ustawowe i wykonawcze przewidują bardziej rygorystyczne zasady tymczasowego pełnienia obowiązków, jednorazowego dostępu do informacji niejawnych lub dostępu do takich informacji w sytuacjach nadzwyczajnych, procedury przewidziane w niniejszej sekcji stosowane są wyłącznie w ramach ograniczeń ustalonych w odnośnych przepisach ustawowych i wykonawczych.

41. Komitet ds. Bezpieczeństwa otrzymuje roczne sprawozdanie na temat korzystania z procedur określonych w niniejszej sekcji.

VI. UDZIAŁ W POSIEDZENIACH W RADZIE

42. Z zastrzeżeniem pkt 29, osoby wyznaczone do udziału w tych posiedzeniach Rady lub organów przygotowawczych Rady, podczas których omawiane są informacje oznaczone klauzulą CONFIDENTIEL UE lub wyższą, mogą brać w nich udział tylko po potwierdzeniu statusu ich PBO. W przypadku delegatów certyfikat potwierdzający posiadanie przez nich poświadczenia bezpieczeństwa osobowego lub inny dowód posiadania przez nich PBO przesyłany jest przez odpowiednie organy do Biura ds. Bezpieczeństwa SGR lub, w sytuacjach wyjątkowych, przedstawiany jest przez samego delegata. W stosownych przypadkach można zastosować skonsolidowany wykaz nazwisk, przedstawiając odnośne dowody posiadania PBO.

43. Jeżeli z powodów bezpieczeństwa wycofane zostaje krajowe PBO osoby, której obowiązki wymagają uczestnictwa w posiedzeniach Rady lub organów przygotowawczych Rady, właściwy organ informuje o tym SGR.

VII. SPOSOBNOŚĆ DOSTĘPU DO INFORMACJI NIEJAWNYCH UE

44. Osoby, które mają zostać zatrudnione w warunkach dających sposobność dostępu do informacji o klauzuli CONFIDENTIEL UE lub wyższej, zostają odpowiednio sprawdzone pod względem bezpieczeństwa lub przez cały czas towarzyszy im eskorta.

45. Kurierzy, strażnicy i eskorta są sprawdzani pod względem bezpieczeństwa do odnośnego poziomu lub w inny sposób odpowiednio sprawdzani zgodnie z krajowymi przepisami ustawowymi i wykonawczymi, informowani o procedurach bezpieczeństwa w zakresie ochrony informacji niejawnych UE oraz instruowani o obowiązku ochrony informacji, które im powierzono.

ZAŁĄCZNIK II

BEZPIECZEŃSTWO FIZYCZNE

I. WPROWADZENIE

1. Niniejszy załącznik zawiera przepisy dotyczące wprowadzania w życie art. 8. Określa on minimalne wymogi w zakresie fizycznej ochrony obiektów, budynków, biur, pomieszczeń i innych stref, w których informacje niejawne UE są wykorzystywane do pracy i przechowywane, w tym stref, w których znajdują się systemy CIS.

2. Środki bezpieczeństwa fizycznego mają na celu zapobieżenie nieuprawnionemu dostępowi do informacji niejawnych UE przez:

   (a) zapewnienie właściwego wykorzystywania informacji niejawnych UE do pracy i ich właściwego przechowywania;

   (b) umożliwienie podziału pracowników pod względem dostępu do informacji niejawnych UE według zasady ograniczonego dostępu i, w odpowiednich przypadkach, sprawdzenia pod względem bezpieczeństwa;

   (c) powstrzymywanie od podejmowania nieuprawnionych działań, udaremnianie i wykrywanie ich; oraz

   (d) uniemożliwienie lub opóźnienie wtargnięcia intruzów w sposób niezauważony lub z użyciem siły.

II. WYMOGI I ŚRODKI BEZPIECZEŃSTWA FIZYCZNEGO

3. Środki bezpieczeństwa fizycznego dobiera się na podstawie oceny zagrożenia przeprowadzonej przez właściwe organy. SGR i państwa członkowskie stosują w swoich obiektach system kontroli ryzyka służący ochronie informacji niejawnych UE, aby zapewnić poziom ochrony fizycznej proporcjonalny do szacowanego ryzyka. System kontroli ryzyka uwzględnia wszystkie istotne czynniki, a w szczególności:

(a) klauzulę informacji niejawnych UE;

(b) postać i ilość informacji niejawnych UE, z uwzględnieniem faktu, że duże ilości informacji niejawnych UE lub ich zbiór mogą wymagać zastosowania bardziej rygorystycznych środków ochronnych;

(c) otoczenie i strukturę budynków lub stref, w których znajdują się informacje niejawne UE; oraz

(d) oszacowane zagrożenie ze strony służb wywiadowczych, których celem są UE lub państwa członkowskie, oraz zagrożenie sabotażem, terroryzmem, działalnością wywrotową lub inną działalnością przestępczą;

4. Stosując koncepcję głębokiej obrony, właściwa władza bezpieczeństwa określa właściwe połączenie środków bezpieczeństwa fizycznego, które należy zastosować. Mogą one obejmować jeden z poniższych środków lub większą ich liczbę:

(a) ogrodzenie: bariera fizyczna, która wyznacza granice strefy wymagającej ochrony;

(b) systemy wykrywania włamań (IDS): IDS można stosować w celu podwyższenia poziomu bezpieczeństwa, jaki daje ogrodzenie, a w pomieszczeniach i budynkach w celu zastąpienia lub wsparcia pracowników ochrony;

(c) kontrola wstępu: kontrola wstępu może obejmować teren, budynek lub budynki znajdujące się na danym terenie lub też strefy lub pomieszczenia wewnątrz budynku. Kontrolę można prowadzić za pomocą środków elektronicznych, środków elektromechanicznych, za pośrednictwem pracowników ochrony lub recepcjonistów lub za pomocą wszelkich innych środków fizycznych;

(d) pracownicy ochrony: przeszkoleni, nadzorowani, a w razie konieczności odpowiednio sprawdzeni pod względem bezpieczeństwa pracownicy ochrony mogą być zatrudniani, między innymi w celu powstrzymania osób planujących niezauważone przedostanie się na dany teren;

(e) telewizja przemysłowa (CCTV): CCTV może być stosowana przez pracowników ochrony w celu sprawdzania incydentów i sygnałów alarmowych pochodzących z IDS na rozległych terenach lub na ogrodzeniach;

(f) oświetlenie ochronne: oświetlenie ochronne może być stosowane w celu powstrzymania potencjalnych intruzów, a ponadto w celu zapewnienia oświetlenia koniecznego do prowadzenia skutecznego nadzoru bezpośrednio przez pracowników ochrony lub pośrednio za pomocą systemu CCTV; oraz

(g) wszelkie inne stosowne środki fizyczne służące powstrzymywaniu osób nieupoważnionych od wstępu na dany teren lub wykrywaniu takich przypadków lub też zapobiegające utracie informacji niejawnych UE lub narażeniu na szwank ich bezpieczeństwa.

5. Właściwy organ może być uprawniony do przeszukiwania osób przy wejściu i wyjściu, co ma stanowić środek odstraszający przed niedozwolonym wnoszeniem materiałów lub niedozwolonym wynoszeniem informacji niejawnych UE z obiektów lub budynków.

6. Kiedy istnieje ryzyko podglądu informacji niejawnych UE, także tylko przypadkowego, podejmuje się stosowne działania w celu zlikwidowania takiego ryzyka.

7. W przypadku nowych obiektów wymogi dotyczące bezpieczeństwa fizycznego i specyfikacje dotyczące ich stosowania określane są w ramach planowania i projektowania tych obiektów. W przypadku obiektów już istniejących wymogi dotyczące bezpieczeństwa fizycznego stosowane są w największym możliwym zakresie.

III. SPRZĘT SŁUŻĄCY DO FIZYCZNEJ OCHRONY INFORMACJI NIEJAWNYCH UE

8. Przy zakupie sprzętu służącego do fizycznej ochrony informacji niejawnych UE (takiego jak zabezpieczone pojemniki, niszczarki, zamki do drzwi, elektroniczne systemy kontroli dostępu, IDS, systemy alarmowe itp.) właściwe władze bezpieczeństwa dbają o to, by sprzęt ten spełniał zatwierdzone normy techniczne i minimalne wymogi.

9. Specyfikacje techniczne sprzętu, który ma być wykorzystywany do fizycznej ochrony informacji niejawnych UE, określane są w wskazówek technicznych dotyczących bezpieczeństwa, które zatwierdza Komitet ds. Bezpieczeństwa.

10. Systemy bezpieczeństwa są poddawane regularnym kontrolom, a sprzęt – regularnej konserwacji. Podczas konserwacji uwzględnia się wyniki kontroli, aby zapewnić dalsze optymalne działanie sprzętu.

11. Podczas każdej kontroli przeprowadza się ocenę skuteczności poszczególnych środków bezpieczeństwa oraz całego systemu bezpieczeństwa.

IV. STREFY CHRONIONE FIZYCZNIE

12. Ustanawia się dwa rodzaje stref chronionych fizycznie lub ich krajowych odpowiedników, w których informacje niejawne UE są objęte ochroną fizyczną:

    - strefy administracyjne; oraz

    - strefy zabezpieczone (w tym strefy zabezpieczone technicznie).

    W całym niniejszej decyzji wszystkie odniesienia do stref administracyjnych i stref zabezpieczonych, w tym stref zabezpieczonych technicznie, należy rozumieć jako odnoszące się także do ich krajowych odpowiedników.

13. Właściwe władze bezpieczeństwa stwierdzają, czy dana strefa spełnia wymogi potrzebne do uznania jej za strefę administracyjną, strefę zabezpieczoną lub strefę zabezpieczoną technicznie.

14. W przypadku stref administracyjnych:

    (a) należy wyraźnie określić granice umożliwiające kontrolę osób i, jeżeli to możliwe, pojazdów;

(b) dostęp bez eskorty umożliwia się tylko osobom, które są odpowiednio upoważnione przez właściwy organ; oraz

(c) wszystkim innym osobom musi przez cały czas towarzyszyć eskorta lub należy je poddać równoważnej kontroli.

15. W przypadku stref zabezpieczonych:

(a) należy wyraźnie określić zabezpieczone granice, na których wszelkie wejścia i wyjścia kontrolowane są za pomocą przepustki lub systemu rozpoznawania osób;

(b) wstęp bez eskorty umożliwia się tylko osobom sprawdzonym pod względem bezpieczeństwa i wyraźnie uprawnionym do wejścia do danej strefy ze względu na zasadę ograniczonego dostępu;

(c) wszystkim innym osobom musi przez cały czas towarzyszyć eskorta lub należy je poddać równoważnej kontroli.

16. Jeżeli wejście do strefy zabezpieczonej jest w praktyce równoznaczne z bezpośrednim dostępem do informacji niejawnych znajdujących się w tej strefie, zastosowanie mają następujące dodatkowe wymogi:

(a) wyraźnie wskazuje się najwyższą klauzulę tajności, którą przyznano informacjom zwykle przechowywanym w tej strefie;

(b) wszystkie osoby wchodzące do tej strefy muszą posiadać specjalne upoważnienie do wejścia do tej strefy, przez cały czas towarzyszyć im musi eskorta i muszą być stosownie sprawdzone pod względem bezpieczeństwa, chyba że podjęte zostały kroki służące dopilnowaniu, aby nie był możliwy dostęp do informacji niejawnych UE.

17. Strefy zabezpieczone chronione przed podsłuchem uznawane są za strefy zabezpieczone technicznie. Do takich stref zastosowane mają następujące dodatkowe wymogi:

(a) są one wyposażone w IDS, są zamknięte na zamek, gdy nikt w nich nie przebywa, i chronione, gdy ktoś w nich przebywa. Wszystkie klucze podlegają kontroli zgodnie z częścią VI;

(b) wszystkie osoby wchodzące do takich stref lub materiały tam wnoszone podlegają kontroli;

(c) strefy takie podlegają regularnym kontrolom fizycznym lub technicznym zgodnie z wymogami właściwej władzy bezpieczeństwa. Kontrole takie przeprowadza się także po każdorazowym nieuprawnionym wejściu do strefy lub podejrzeniu, że takie wejście miało miejsce; oraz

(d) w strefach takich nie mogą się znajdować niezatwierdzone linie komunikacyjne, niezatwierdzone telefony, inne niezatwierdzone urządzenia komunikacyjne ani sprzęt elektryczny lub elektroniczny.

18. Niezależnie od pkt 17 ppkt d), zanim urządzenia komunikacyjne i sprzęt elektryczny lub elektroniczny zostaną użyte w strefach, w których odbywają się posiedzenia lub prowadzone są prace związane z wykorzystaniem informacji o klauzuli SECRET UE i wyższej, a także jeżeli ocenia się, że istnieje wysokie zagrożenie dla informacji niejawnych UE, urządzenia i sprzęt taki zostają najpierw zbadane przez właściwe władze bezpieczeństwa w celu dopilnowania, aby żadne zrozumiałe informacje nie zostały nieumyślnie lub nielegalnie przekazane przez taki sprzęt poza granicę strefy zabezpieczonej.

19. Strefy zabezpieczone, w których nie pracują w systemie całodobowym pracownicy pełniący dyżur, są w odpowiednich przypadkach poddawane kontroli na koniec normalnych godzin pracy i w przypadkowych odstępach czasu poza tymi godzinami, chyba że zaopatrzone są w IDS.

20. Strefy zabezpieczone oraz strefy zabezpieczone technicznie mogą być tworzone tymczasowo na terenie stref administracyjnych w celu zorganizowania niejawnego posiedzenia lub w jakimkolwiek innym podobnym celu.

21. Dla każdej strefy zabezpieczonej opracowywane są operacyjne procedury bezpieczeństwa określające:

(a) klauzulę informacji niejawnych UE, które można wykorzystywać do pracy i przechowywać w tej strefie;

(b) środki nadzoru i ochrony, które należy stosować;

(c) osoby upoważnione do wstępu do strefy bez eskorty ze względu na zasadę ograniczonego dostępu i ich sprawdzenie pod względem bezpieczeństwa;

(d) w odpowiednich przypadkach procedury dotyczące eskort lub ochrony informacji niejawnych UE, jeżeli zezwala się na wstęp do strefy innym osobom;

(e) wszelkie inne odnośne środki i procedury.

22. W ramach stref zabezpieczonych są budowane wzmocnione pomieszczenia. Ściany, podłogi, sufity, okna i zamykane na zamek drzwi zatwierdzane są przez właściwe władze bezpieczeństwa i zapewniają ochronę równoważną zabezpieczonemu pojemnikowi zatwierdzonemu do celów przechowywania informacji niejawnych UE o tym samym poziomie klauzuli tajności.

V. FIZYCZNE ŚRODKI OCHRONNE NA POTRZEBY PRACY Z WYKORZYSTANIEM INFORMACJI NIEJAWNYCH UE I ICH PRZECHOWYWANIA

23. Jeżeli informacje niejawne UE zaszyfrowane są za pomocą środków elektronicznych chronionych przy użyciu produktów kryptograficznych zatwierdzonych zgodnie z art. 9 ust. 6, środek ten i jego zawartość (tj. kryptogram) mogą być przetwarzane i przechowywane jako informacje jawne. Rada zatwierdza politykę bezpieczeństwa w sprawie zapewnienia właściwej odpowiedzialności za takie informacje.

24. Praca z wykorzystaniem informacji niejawnych UE o klauzuli RESTREINT UE może się odbywać:

(a) w strefie zabezpieczonej;

(b) w strefie administracyjnej, pod warunkiem że informacje niejawne UE są chronione przed dostępem osób nieupoważnionych; lub

(c) poza strefą zabezpieczoną lub strefą administracyjną, pod warunkiem że posiadacz informacji zobowiązał się do zastosowania środków równoważnych określonych w instrukcjach bezpieczeństwa wydanych przez właściwą władzę bezpieczeństwa służących dopilnowaniu, aby nieupoważnione osoby nie miały dostępu do informacji niejawnych UE.

25. Informacje niejawne UE o klauzuli RESTREINT UE przechowywane są w odpowiednim do tego celu, zamkniętym na zamek meblu biurowym w strefie administracyjnej lub strefie zabezpieczonej.

Mogą być tymczasowo przechowywane poza strefą zabezpieczoną lub strefą administracyjną, pod warunkiem że posiadacz informacji zobowiązał się do zastosowania środków równoważnych określonych w instrukcjach bezpieczeństwa wydanych przez właściwą władzę bezpieczeństwa.

26. Praca z wykorzystaniem informacji niejawnych UE o klauzuli CONFIDENTIEL UE lub SECRET UE może się odbywać:

(a) w strefie zabezpieczonej;

(b) w strefie administracyjnej, pod warunkiem że informacje niejawne UE są chronione przed dostępem osób nieupoważnionych; lub

(c) wyjątkowo poza strefą zabezpieczoną lub strefą administracyjną, pod warunkiem że posiadacz informacji:

(i) zobowiązał się do zastosowania środków równoważnych określonych w instrukcjach bezpieczeństwa wydanych przez właściwą władzę bezpieczeństwa służących dopilnowaniu, aby nieupoważnione osoby nie miały dostępu do informacji niejawnych UE; oraz

(ii) przechowuje informacje niejawne UE przez cały czas pod swoją kontrolą; oraz

(iii) w przypadku dokumentów w formie papierowej – powiadomił o tym fakcie właściwą kancelarię tajną.

27. Informacje niejawne UE o klauzuli CONFIDENTIEL UE lub SECRET UE przechowywane są w strefie zabezpieczonej w zabezpieczonym pojemniku lub wzmocnionym pomieszczeniu.

28. Praca z wykorzystaniem informacji niejawnych UE oznaczonych klauzulą TRES SECRET UE odbywa się w strefie zabezpieczonej.

29. Informacje niejawne UE o klauzuli TRES SECRET UE przechowywane są w strefie zabezpieczonej, przy czym musi zostać spełniony jeden z następujących warunków:

(a) są one przechowywane w zabezpieczonym pojemniku, zgodnie z pkt 8, wyposażonym w co najmniej jedno z następujących zabezpieczeń dodatkowych:

(i) stała ochrona lub kontrole przez sprawdzonych pod względem bezpieczeństwa pracowników ochrony lub pracowników pełniących dyżur;

(ii) zatwierdzony IDS w połączeniu z personelem reagowania odpowiedzialnym za bezpieczeństwo; lub

(b) są one przechowywane we wzmocnionym pomieszczeniu wyposażonym w IDS oraz obsługiwanym przez personel reagowania odpowiedzialny za bezpieczeństwo.

30. Przed opuszczeniem jakiejkolwiek strefy, w której znajdują się informacje niejawne UE, osoby, w których posiadaniu znajdują się te informacje, sprawdzają, czy są one bezpiecznie przechowywane.

31. Przepisy regulujące przewożenie informacji niejawnych UE poza strefy chronione fizycznie znajdują się w załączniku IV.

VI. KONTROLA KLUCZY I KOMBINACJI SZYFROWYCH WYKORZYSTYWANYCH DO OCHRONY INFORMACJI NIEJAWNYCH UE

32. Właściwa władza bezpieczeństwa określa procedury zarządzania kluczami i kombinacjami szyfrowymi do biur, pomieszczeń, wzmocnionych pomieszczeń i zabezpieczonych pojemników.

33. Klucze i kombinacje szyfrowe podlegają środkom ochrony i kontroli nie mniej rygorystycznym niż środki mające zastosowanie do informacji niejawnych UE, do których umożliwiają dostęp.

34. Kombinacje szyfrowe są zapamiętywane przez jak najmniejszą liczbę osób, które muszą je znać. Kombinacje szyfrowe do zabezpieczonych pojemników, w których przechowywane są informacje niejawne UE, są zmieniane:

(a) przy każdej zmianie pracowników znających kombinację szyfrową;

(b) w każdym przypadku, gdy następuje rzeczywiste lub domniemane narażenie na szwank bezpieczeństwa informacji; oraz

(c) co najmniej co 12 miesięcy.

ZAŁĄCZNIK III

OCHRONA INFORMACJI NIEJAWNYCH UE PRZETWARZANYCH W SYSTEMACH ŁĄCZNOŚCI I INFORMACJI

I. WPROWADZENIE

1. Niniejszy załącznik zawiera przepisy dotyczące wprowadzania w życie art. 9.

2. Następujące cechy i koncepcje zabezpieczenia informacji są niezbędne dla bezpieczeństwa i prawidłowego funkcjonowania operacji dokonywanych w ramach CIS:

Autentyczność:	gwarancja, że informacje są prawdziwe i pochodzą z rzetelnych źródeł;
Dostępność:	cecha polegająca na tym, że informacje są dostępne i gotowe do wykorzystania na wniosek uprawnionego podmiotu;
Poufność:	cecha polegająca na tym, że informacje nie są ujawniane nieupoważnionym osobom, podmiotom ani do celów nieuprawnionego przetwarzania;
Integralność:	cecha polegająca na zachowywaniu dokładności i kompletności informacji i zasobów;
Niezaprzeczalność:	możliwość udowodnienia, że działanie lub wydarzenie miało miejsce, aby następnie nie można było zaprzeczyć wystąpieniu tego działania lub wydarzenia.

II. ZASADY ZABEZPIECZANIA INFORMACJI

3. Przedstawione poniżej przepisy stanowią podstawę bezpieczeństwa wszelkich systemów CIS, w ramach których odbywa się praca z wykorzystaniem informacji niejawnych UE. Szczegółowe wymogi dotyczące wdrażania tych przepisów są zdefiniowane w ramach polityk bezpieczeństwa w zakresie zabezpieczania informacji oraz w wskazówkach technicznych dotyczących bezpieczeństwa.

Kontrola ryzyka naruszenia bezpieczeństwa

4. Kontrola ryzyka naruszenia bezpieczeństwa stanowi integralną część definiowania, rozwijania, obsługiwania i konserwacji CIS. Cztery etapy kontroli ryzyka (ocena, zmniejszanie, akceptacja i powiadamianie) są wielokrotnie powtarzane wspólnie przez przedstawicieli właścicieli systemu, organy odpowiedzialne za projekt, organy operacyjne oraz organy zatwierdzające bezpieczeństwo, w ramach sprawdzonego, przejrzystego i w pełni zrozumiałego procesu oceny ryzyka. Zakres stosowania CIS oraz jego zasobów jest jasno definiowany na początku procesu kontroli ryzyka.

5. Właściwe organy przeprowadzają przegląd potencjalnych zagrożeń dla CIS i posiadają aktualne i dokładne oceny ryzyka, odzwierciedlające aktualne środowisko operacyjne. Stale uaktualniają swoją wiedzę na temat kwestii związanych z narażeniem na zagrożenia i dokonują okresowych przeglądów oceny narażenia, aby dostosować się do zmieniających się technologii informacyjnych.

6. Celem zmniejszania ryzyka naruszenia bezpieczeństwa jest zastosowanie zestawu środków bezpieczeństwa prowadzących do osiągnięcia zadowalającej równowagi między wymaganiami użytkownika, kosztami a szczątkowym ryzykiem naruszenia bezpieczeństwa.

7. Szczególne wymogi, skala i stopień szczegółowości określone przez odpowiednie SAA do celów przyznania akredytacji CIS są proporcjonalne do szacowanego ryzyka z uwzględnieniem wszystkich odpowiednich czynników, w tym klauzuli tajności informacji niejawnych UE przetwarzanych w danym CIS. Akredytacja obejmuje oficjalne oświadczenie o ryzyku szczątkowym oraz akceptację ryzyka szczątkowego przez odpowiedzialny organ.

Bezpieczeństwo na wszystkich etapach istnienia systemu

8. Zapewnianie bezpieczeństwa jest wymogiem obowiązującym na wszystkich etapach istnienia CIS, od jego uruchomienia do wycofania z użytkowania.

9. Dla każdego etapu istnienia CIS określana jest rola i interakcja każdego z podmiotów związanych z CIS w odniesieniu do jego bezpieczeństwa.

10. Wszystkie CIS wraz z technicznymi i innymi środkami bezpieczeństwa są podczas procedury akredytacyjnej poddawane testom bezpieczeństwa, aby zapewnić osiągnięcie odpowiedniego stopnia zabezpieczenia oraz sprawdzić, czy są one prawidłowo wdrożone, zintegrowane i skonfigurowane.

11. Oceny bezpieczeństwa, kontrole i przeglądy przeprowadzane są okresowo w fazie operacyjnej oraz podczas konserwacji CIS, jak również przy pojawieniu się nadzwyczajnych okoliczności.

12. Dokumentacja bezpieczeństwa CIS ewoluuje podczas wszystkich etapów jego istnienia na zasadzie integralnej części procesu zmian i zarządzania konfiguracjami.

Najlepsze wzorce

13. SGR i państwa członkowskie współpracują, aby opracować najlepsze wzorce ochrony informacji niejawnych UE, z których korzysta się podczas pracy w ramach CIS. Wytyczne w zakresie najlepszych wzorców zawierają techniczne, fizyczne, organizacyjne i proceduralne środki bezpieczeństwa dotyczące CIS o sprawdzonej skuteczności w zapobieganiu danym zagrożeniom i narażeniom.

14. Ochrona informacji niejawnych UE wykorzystywanych podczas pracy w ramach CIS opiera się na doświadczeniach podmiotów zaangażowanych w zabezpieczanie informacji, zarówno w UE, jak i poza nią.

15. Rozpowszechnianie, a następnie wdrażanie najlepszych wzorców pomaga w osiągnięciu równoważnego poziomu bezpieczeństwa różnych CIS, eksploatowanych przez SGR i państwa członkowskie, które pracują z wykorzystaniem informacji niejawnych UE.

Głęboka obrona

16. Aby zmniejszyć ryzyko zagrażające CIS, wdrażany jest pakiet technicznych i innych środków bezpieczeństwa o strukturze różnych poziomów obrony. Poziomy te obejmują:

(a) *Powstrzymywanie*: środki bezpieczeństwa ukierunkowane na odwiedzenie wrogów od zaplanowania ataku na CIS;

(b) *Zapobieganie*: środki bezpieczeństwa ukierunkowane na udaremnienie lub powstrzymanie ataku na CIS;

(c) *Wykrywanie*: środki bezpieczeństwa ukierunkowane na ujawnienie ataku na CIS;

(d) *Odporność*: środki bezpieczeństwa ukierunkowane na ograniczenie skutków ataku, tak by dotknęły one jak najmniejszą ilość informacji lub zasobów CIS, oraz na zapobieżenie dalszym szkodom; oraz

(e) *Usuwanie skutków*: środki bezpieczeństwa ukierunkowane na odzyskanie bezpiecznego statusu CIS.

Rygorystyczność takich środków bezpieczeństwa ustalana jest na podstawie oceny ryzyka.

17. Właściwe organy dbają o to, by były w stanie reagować na incydenty, które mogą przekraczać granice poszczególnych organizacji i państw, by skoordynować reakcje i dzielić się informacjami o tych incydentach i związanym z nimi ryzyku (zdolności do reagowania na sytuacje nadzwyczajne w ramach systemów komputerowych).

Zasada minimalizmu i najniższego uprzywilejowania

18. Aby zapobiec niepotrzebnemu ryzyku, stosowane będą wyłącznie funkcje, urządzenia i usługi niezbędne do spełnienia wymogów operacyjnych.

19. Aby ograniczyć szkody wynikające z wypadków, błędów lub korzystania z zasobów systemu łączności i informacji bez odpowiedniego upoważnienia, użytkownicy CIS oraz procesy zautomatyzowane otrzymują wyłącznie taki dostęp i takie przywileje i upoważnienia, jakie są im potrzebne do wykonywania zadań.

20. Procedury rejestracji stosowane w razie konieczności w ramach CIS sprawdzane są jako element procedury akredytacji.

Świadomość zabezpieczania informacji

21. Świadomość ryzyka i dostępnych środków bezpieczeństwa stanowi pierwszą linię obrony bezpieczeństwa CIS i sieci. W szczególności wszyscy członkowie personelu związani z CIS na poszczególnych etapach jego istnienia, w tym użytkownicy, powinni zrozumieć:

    (a) że niedopatrzenia w zakresie bezpieczeństwa mogą znacznie zaszkodzić CIS i sieciom, w ramach których odbywa się praca z wykorzystaniem informacji niejawnych UE;

    (b) potencjalne szkody, jakie mogą ponieść inne podmioty w związku z podłączeniem do systemów lub sieci i współzależnością; oraz

    (c) że osobiście ponoszą odpowiedzialność i są rozliczani za bezpieczeństwo CIS zgodnie z pełnionymi przez siebie funkcjami w tych systemach i procesach.

22. Aby zrozumieć obowiązki związane z bezpieczeństwem, wszyscy członkowie personelu, w tym wyższe kierownictwo i użytkownicy CIS, przechodzą obowiązkowe szkolenia mające na celu edukację i zdobycie wiedzy w zakresie zabezpieczenia informacji.

Ocena i zatwierdzanie produktów służących bezpieczeństwu systemów informatycznych

23. Wymagany stopień zabezpieczenia, jaki zapewniają środki bezpieczeństwa, określony jako poziom zabezpieczenia, określa się zgodnie z wynikami procesu kontroli ryzyka i zgodnie z odpowiednimi politykami i wskazówkami technicznymi w dziedzinie bezpieczeństwa.

24. Poziom zabezpieczenia sprawdzany jest przy użyciu uznanych na szczeblu międzynarodowym lub zatwierdzonych na szczeblu krajowym procesów i metod. Obejmują one przede wszystkim ocenę, kontrole i audyt.

25. Urządzenia kryptograficzne służące ochronie informacji niejawnych UE są oceniane i zatwierdzane przez krajowy CAA danego państwa członkowskiego.

26. Przed zaleceniem Radzie lub SG/WP zatwierdzenia produktów kryptograficznych, zgodnie z art. 9 ust. 6, produkty te muszą uzyskać pozytywny wynik podczas zewnętrznej oceny dokonywanej przez wykwalifikowany organ oceny produktów kryptograficznych (AQUA) państwa członkowskiego, które nie jest zaangażowane w projektowanie ani wytwarzanie tego sprzętu. Wymagany stopień szczegółowości oceny zewnętrznej zależy od przewidywanego najwyższego poziomu klauzuli informacji niejawnych UE, które mają być chronione za pomocą tych produktów. Rada zatwierdza politykę bezpieczeństwa dotyczącą oceny i zatwierdzania produktów kryptograficznych.

27. Jeżeli uzasadniają to określone względy operacyjne, Rada lub, w stosownych przypadkach, SG/WP mogą znieść na zalecenie Komitetu ds. Bezpieczeństwa wymogi wynikające z pkt 25 lub 26 i udzielić tymczasowego zatwierdzenia na dany okres zgodnie z procedurą określoną w art. 9 ust. 6.

28. AQUA jest organem zatwierdzania produktów kryptograficznych (CAA) państwa członkowskiego, który na podstawie kryteriów ustalonych przez Radę otrzymał akredytację, aby przeprowadzić drugą ocenę urządzeń kryptograficznych służących ochronie informacji niejawnych UE.

29. Rada zatwierdza politykę bezpieczeństwa dotyczącą kwalifikowania i zatwierdzania niekryptograficznych produktów służących bezpieczeństwu systemów informatycznych.

Przekazywanie w strefie zabezpieczonej

30. Niezależnie od przepisów niniejszej decyzji, gdy przekazywanie informacji niejawnych UE ogranicza się do stref zabezpieczonych, można je dystrybuować w postaci niezaszyfrowanej lub zaszyfrować je na niższym poziomie na podstawie wyników procesu kontroli ryzyka i z zastrzeżeniem zatwierdzenia przez SAA.

Bezpieczne połączenia międzysystemowe CIS

31. Do celów niniejszej decyzji połączenie międzysystemowe oznacza bezpośrednie połączenie co najmniej dwóch systemów informatycznych w celu wspólnego korzystania z danych i innych zasobów informacyjnych (np. łączności) w sposób jednokierunkowy lub wielokierunkowy.

32. Dany CIS traktuje każdy system informatyczny przyłączony połączeniem międzysystemowym jako niewzbudzający zaufania i stosuje środki ochronne, aby kontrolować wymianę informacji niejawnych.

33. Wszystkie połączenia międzysystemowe CIS z innym systemem informatycznym spełniają następujące podstawowe wymogi:

    (a) wymogi dotyczące działania i wymogi operacyjne takich połączeń międzysystemowych są określane i zatwierdzane przez właściwe organy;

(b) połączenie międzysystemowe przechodzi proces kontroli ryzyka i akredytacji oraz wymaga zatwierdzenia przez właściwe organy akredytacji bezpieczeństwa; oraz

(c) na granicach wszystkich CIS stosowane są usługi zabezpieczania granic (BPS).

34. Pomiędzy CIS posiadającym akredytację a siecią niezabezpieczoną lub publiczną brak jest połączeń międzysystemowych z wyjątkiem sytuacji, w których w ramach CIS zainstalowano w tym celu zatwierdzone BPS między CIS a siecią niezabezpieczoną lub publiczną. Środki bezpieczeństwa dotyczące takich połączeń międzysystemowych są poddawane przeglądowi przez właściwy organ ds. zabezpieczania informacji i zatwierdzane przez właściwy SAA.

Gdy sieć niezabezpieczona lub publiczna wykorzystywana jest wyłącznie jako nośnik, a dane zostały zaszyfrowane przy wykorzystaniu produktu kryptograficznego zatwierdzonego zgodnie z art. 9, takiego połączenia nie uznaje się za połączenie międzysystemowe.

35. Bezpośrednie lub kaskadowe połączenie międzysystemowe CIS posiadającego akredytację do pracy z wykorzystaniem informacji o klauzuli TRES SECRET UE/EU TOP SECRET z siecią niezabezpieczoną lub publiczną jest zakazane.

Sytuacje nadzwyczajne

36. Niezależnie od przepisów niniejszej decyzji w sytuacjach nadzwyczajnych, takich jak zbliżający się lub trwający kryzys, konflikt, stan wojny, lub w wyjątkowych sytuacjach operacyjnych można stosować specjalne procedury opisane poniżej:

37. Informacje niejawne UE można przekazywać z wykorzystaniem produktów kryptograficznych zatwierdzonych dla niższego poziomu klauzuli lub w postaci niezaszyfrowanej za zgodą właściwego organu, jeżeli wszelka zwłoka spowodowałaby szkody wyraźnie przewyższające szkody, które mogłoby spowodować ujawnienie materiałów niejawnych, oraz jeżeli:

– nadawca i odbiorca nie posiadają wymaganego urządzenia szyfrującego lub też nie posiadają żadnego urządzenia szyfrującego;

ORAZ

– materiały niejawne nie mogą być dostarczone na czas w inny sposób.

38. Informacje niejawne przekazywane w okolicznościach przedstawionych w pkt 37 nie są opatrzone żadnymi oznaczeniami towarzyszącymi klauzuli ani wskazaniami odróżniającymi je od wiadomości jawnej lub wiadomości, która może być chroniona przy pomocy dostępnego urządzenia szyfrującego. Odbiorcy takich informacji są za pomocą innych środków bezzwłocznie powiadamiani o poziomie klauzuli danej wiadomości.

39. W przypadku stosowania przepisów pkt 37 należy następnie sporządzić sprawozdanie dla właściwych organów i Komitetu ds. Bezpieczeństwa.

III. OBOWIĄZKI ORGANÓW

40. Państwa członkowskie i SGR otrzymują wymienione poniżej zadania dotyczące zabezpieczania informacji. Zadania te nie muszą być skupione w tych samych jednostkach organizacyjnych. Są objęte oddzielnymi mandatami, ale mogą być połączone lub zintegrowane w tej samej jednostce organizacyjnej lub też podzielone na różne jednostki organizacyjne, z zastrzeżeniem uniknięcia wewnętrznych konfliktów interesów lub zadań.

Organ ds. zabezpieczania informacji

41. Organ ds. zabezpieczania informacji odpowiada za:

(a) opracowywanie polityki bezpieczeństwa i technicznych wskazówek dotyczących bezpieczeństwa w zakresie zabezpieczenia informacji oraz za monitorowanie ich skuteczności i adekwatności;

(b) zabezpieczanie informacji technicznych związanych z produktami kryptograficznymi i zarządzanie tymi informacjami;

(c) dopilnowanie, by środki zabezpieczania informacji wybrane do ochrony informacji niejawnych UE były zgodne z odnośnymi politykami dotyczącymi kryteriów przydatności i wyboru;

(d) dopilnowanie, by wybór produktów kryptograficznych następował zgodnie z politykami dotyczącymi kryteriów przydatności i wyboru;

(e) koordynowanie szkoleń i upowszechnianie wiedzy na temat zabezpieczenia informacji;

(f) dopilnowanie, by CIS były dostosowane do polityk bezpieczeństwa i technicznych wskazówek dotyczących bezpieczeństwa TEMPEST (organ ds. TEMPEST);

(g) konsultowanie się z dostawcą systemu, podmiotami odpowiedzialnymi za bezpieczeństwo i przedstawicielami użytkowników w związku z polityką bezpieczeństwa i technicznymi wskazówkami dotyczącymi bezpieczeństwa w zakresie zabezpieczania informacji; oraz

(h) zapewnianie odpowiednich ekspertów w składzie Komitetu ds. Bezpieczeństwa zajmującym się poddziedziną zabezpieczania informacji.

Organ zatwierdzania produktów kryptograficznych

42. Organ zatwierdzania produktów kryptograficznych (CAA) odpowiada za dopilnowanie, by produkty kryptograficzne były zgodne z, odpowiednio, krajową polityką kryptograficzną i polityką kryptograficzną Rady. Wydaje zgodę na to, by dany produkt kryptograficzny w swoim środowisku operacyjnym chronił informacje niejawne UE do określonego poziomu klauzuli tajności. Jeśli chodzi o państwa członkowskie, CAA jest dodatkowo odpowiedzialny za ocenę produktów kryptograficznych.

Organ ds. rozpowszechniania produktów kryptograficznych

43. Organ ds. rozpowszechniania produktów kryptograficznych (CDA) odpowiada za:

(a) zarządzanie materiałami kryptograficznymi UE i przyjęcie za nie odpowiedzialności;

(b) dopilnowanie, by stosowano odpowiednie procedury i stworzono kanały umożliwiające przyjmowanie odpowiedzialności za wszystkie materiały kryptograficzne UE, bezpieczną pracę z ich wykorzystaniem, ich przechowywanie i rozpowszechnianie; oraz

(c) zapewnianie przekazywania materiałów kryptograficznych UE między osobami lub służbami korzystającymi z tych materiałów.

Organ ds. akredytacji bezpieczeństwa

44. SAA jest odpowiedzialny za:

(a) dopilnowanie, by CIS był zgodny z odnośnymi politykami bezpieczeństwa i technicznymi wskazówkami dotyczącymi bezpieczeństwa, dostarczając poświadczenie zatwierdzenia CIS do celów pracy z wykorzystaniem informacji niejawnych UE do określonego poziomu klauzuli tajności w jego środowisku operacyjnym; w poświadczeniu określa się warunki akredytacji oraz kryteria, które muszą być spełnione, by konieczne było ponowne zatwierdzenie;

(b) utworzenie procesu akredytacji bezpieczeństwa, zgodnie z odnośnymi politykami, z określonymi warunkami zatwierdzenia CIS pod nadzorem tego organu;

(c) określanie strategii akredytacji bezpieczeństwa przez ustalenie stopnia szczegółowości procedury akredytacji proporcjonalnego do wymaganego poziomu zabezpieczenia;

(d) analizowanie i zatwierdzanie dokumentacji związanej z bezpieczeństwem, w tym oświadczeń o kontroli ryzyka i o ryzyku szczątkowym, oświadczeń o wymogach bezpieczeństwa dotyczących danego systemu (zwanych dalej „SSRS"), dokumentacji związanej z weryfikacją zapewnienia bezpieczeństwa oraz wdrożenia procedur bezpieczeństwa operacyjnego (zwanych dalej „SecOP"), jak również dopilnowanie, by dokumentacja ta była zgodna z polityką i zasadami bezpieczeństwa Rady;

(e) sprawdzanie wdrażania środków bezpieczeństwa w odniesieniu do CIS przez dokonywanie ocen, inspekcji lub przeglądów bezpieczeństwa czy też wspieranie takich działań;

(f) zatwierdzanie wymogów bezpieczeństwa (np. poziomów sprawdzania pracowników) w przypadku stanowisk o szczególnie wrażliwym charakterze w odniesieniu do CIS;

(g) zatwierdzanie wyboru produktów kryptograficznych i produktów klasy TEMPEST wykorzystywanych do zapewnienia bezpieczeństwa CIS;

(h) zatwierdzanie lub w odpowiednich przypadkach uczestniczenie we wspólnym zatwierdzaniu międzysystemowego połączenia CIS z innymi CIS; oraz

(i) konsultowanie się z dostawcą systemu, podmiotami odpowiedzialnymi za bezpieczeństwo i przedstawicielami użytkowników w związku z kontrolą ryzyka naruszenia bezpieczeństwa, w szczególności z ryzykiem szczątkowym, jak również warunkami i okolicznościami poświadczenia zatwierdzenia.

45. Organ ds. akredytacji bezpieczeństwa SGR jest odpowiedzialny za przyznawanie akredytacji wszystkim CIS działającym pod nadzorem SGR.

46. Odpowiedni SAA państwa członkowskiego jest odpowiedzialny za przyznawanie akredytacji CIS oraz jego częściom składowym działającym pod nadzorem danego państwa członkowskiego.

47. Wspólna Rada ds. Akredytacji Bezpieczeństwa (SAB) jest odpowiedzialna za wydawanie akredytacji CIS działającym pod nadzorem zarówno organu ds. akredytacji bezpieczeństwa SGR, jak i SAA państw członkowskich. W skład tej rady wchodzi po jednym przedstawicielu SAA z każdego państwa członkowskiego, a w jej obradach uczestniczy przedstawiciel SAA z Komisji. Inne podmioty posiadające połączenia z danym CIS są zapraszane do uczestnictwa w obradach, gdy omawiany jest ten system.

Obradom SAB przewodniczy przedstawiciel organu ds. akredytacji bezpieczeństwa SGR. SAB podejmuje decyzje na zasadzie konsensusu przedstawicieli SAA z instytucji, państw członkowskich i innych podmiotów posiadających połączenia z danym CIS. SAB sporządza okresowe sprawozdania ze swojej działalności i przedstawia je Komitetowi ds. Bezpieczeństwa oraz informuje ona komitet o wszystkich poświadczeniach akredytacji.

Operacyjny organ ds. zabezpieczania informacji

48. Operacyjny organ ds. zabezpieczania informacji odpowiada za:

(a) opracowanie dokumentacji bezpieczeństwa zgodnie z politykami bezpieczeństwa i wskazówkami technicznymi dotyczącymi bezpieczeństwa, zwłaszcza SSRS, w tym oświadczenia o ryzyku szczątkowym, SecOP i planu kryptograficznego w ramach procesu akredytacji CIS;

(b) uczestnictwo w wyborze i testowaniu technicznych środków bezpieczeństwa, urządzeń i oprogramowania dla poszczególnych systemów, nadzorowanie ich wdrażania i dopilnowanie, by były one w bezpieczny sposób instalowane, konfigurowane i konserwowane zgodnie z odnośną dokumentacją bezpieczeństwa;

(c) uczestnictwo w wyborze środków bezpieczeństwa i urządzeń klasy TEMPEST, jeżeli jest to wymagane na podstawie SSRS, i dopilnowanie, by były one w bezpieczny sposób instalowane i konserwowane we współpracy z organem ds. zabezpieczania informacji;

(d) monitorowanie wdrażania i stosowania SecOP; w stosownych przypadkach może zlecić właścicielowi systemu operacyjne obowiązki w zakresie bezpieczeństwa;

(e) zarządzanie produktami kryptograficznymi i pracę z ich wykorzystaniem, dopilnowanie nadzoru nad obiektami kryptograficznymi i kontrolowanymi oraz, jeśli jest to wymagane, zapewnienie wytwarzania zmiennych kryptograficznych;

(f) przeprowadzanie przeglądów i testów analizy bezpieczeństwa, w szczególności w celu sporządzenia odnośnych sprawozdań o ryzyku, zgodnie z wymogami SAA;

(g) zapewnianie szkolenia w zakresie zabezpieczenia informacji w odniesieniu do poszczególnych CIS;

(h) wdrażanie środków ochrony sieci w odniesieniu do poszczególnych CIS i stosowanie tych środków.

ZAŁĄCZNIK IV

ZARZĄDZANIE INFORMACJAMI NIEJAWNYMI

I. WPROWADZENIE

1. Niniejszy załącznik zawiera przepisy dotyczące wprowadzania w życie art. 10. Określa on środki administracyjne służące kontroli informacji niejawnych UE na wszystkich etapach ich istnienia, co ma pomóc powstrzymywać od zamierzonego lub przypadkowego narażenia na szwank bezpieczeństwa takich informacji lub ich utraty, wykrywać takie przypadki i usuwać ich skutki.

II. ZARZĄDZENIE KLAUZULAMI TAJNOŚCI

Klauzule tajności i oznaczenia

2. Informacjom nadaje się klauzulę tajności, jeżeli należy chronić ich poufność.

3. Za określenie klauzuli tajności i początkowe rozpowszechnianie informacji odpowiada wytwórca informacji niejawnych UE.

4. Klauzulę tajności informacji niejawnych UE określa się zgodnie z art. 2 ust. 2 niniejszej decyzji i poprzez odniesienie do polityki bezpieczeństwa, która ma być przyjęta zgodnie z art. 3 ust. 3.

5. Klauzulę tajności wskazuje się wyraźnie i poprawnie, niezależnie od tego, czy informacje niejawne UE mają postać przekazu pisemnego, ustnego, elektronicznego czy jakąkolwiek inną formę.

6. Klauzula informacji niejawnych UE nie może być zawyżona ani zaniżona.

7. Poszczególne części danego dokumentu (np. strony, punkty, sekcje, załączniki, dodatki, załączone dokumenty i uzupełnienia) mogą wymagać różnych klauzul i zostają odpowiednio oznaczone, także wtedy, gdy są przechowywane w formie elektronicznej.

8. Ogólna klauzula dokumentu lub akt jest co najmniej tak wysoka, jak klauzula tej części dokumentu, która została oznaczona najwyższą klauzulą tajności. W przypadku zestawiania informacji pochodzących z różnych źródeł sprawdza się ostateczną wersję dokumentu w celu określenia jego ogólnej klauzuli bezpieczeństwa, gdyż może istnieć konieczność nadania mu klauzuli wyższej niż klauzule jego poszczególnych części.

9. W stopniu, w jakim jest to możliwe, dokumenty, których części objęte są różnymi klauzulami, są zestawiane w taki sposób, aby części objęte różnymi klauzulami można było łatwo zidentyfikować i w razie konieczności rozdzielić.

10. Klauzula pisma lub noty zawierających załączniki ma taki poziom jak najwyższa klauzula nadana tym załącznikom. Wytwórca wyraźnie wskazuje, jaka klauzula ma być nadana takiemu pismu lub nocie po ich oddzieleniu od załączników, stosując w tym celu odpowiednie oznaczenie towarzyszące klauzuli, np.:

CONFIDENTIEL UE
Bez załączników RESTREINT UE.

Oznaczenia

11. Oprócz jednego z oznaczeń towarzyszących klauzuli tajności określonych w art. 2 ust. 2 informacje niejawne UE mogą być opatrzone dodatkowymi oznaczeniami, takimi jak:

(a) dane identyfikujące wytwórcę;

(b) wszelkie oznaczenia zastrzegające, kody słowne lub akronimy określające obszar działalności, do którego odnosi się dany dokument, szczególny sposób dystrybucji dokumentu na podstawie zasady ograniczonego dostępu lub ograniczenia w zakresie wykorzystania;

(c) oznaczenia dotyczące możliwości ujawnienia;

(d) w odpowiednich przypadkach data lub konkretne wydarzenie, po których klauzula nadana tym informacjom może zostać obniżona lub zniesiona.

Skrócone oznaczenia towarzyszące klauzulom

12. W celu oznaczenia poziomu klauzuli pojedynczych ustępów tekstu można stosować standardowe skrócone oznaczenia towarzyszące klauzulom. Skróty nie zastępują oznaczeń towarzyszących klauzulom w pełnym brzmieniu.

13. W celu wskazania poziomu klauzuli sekcji lub ciągłych fragmentów tekstu krótszych niż jedna strona w dokumentach niejawnych UE można stosować następujące standardowe skróty:

TRES SECRET UE	TS-UE
SECRET UE	S-UE
CONFIDENTIEL UE	C-UE
RESTREINT UE	R-UE

Tworzenie dokumentów niejawnych UE

14. Przy tworzeniu dokumentu niejawnego UE:

(a) każda strona jest wyraźnie oznaczana klauzulą tajności;

(b) każda strona zostaje opatrzona numerem;

(c) na dokumencie umieszczane są numer referencyjny i temat, który nie stanowi informacji niejawnej, chyba że z jego oznakowania wynika inaczej;

(d) dokument zostaje opatrzony datą;

(e) na każdej stronie dokumentów o klauzuli SECRET UE lub wyższej, które mają zostać rozpowszechnione w kilku kopiach, umieszczany jest numer kopii.

Obniżanie i znoszenie klauzul tajności nadanych informacjom niejawnym UE

15. W momencie wytwarzania informacji niejawnych UE wytwórca wskazuje, o ile to możliwe, czy z daną datą lub w następstwie konkretnego wydarzenia klauzula nadana informacjom niejawnym UE może zostać obniżona lub zniesiona. Wytwórcy informacji oznaczonych klauzulą RESTREINT UE wskazują datę lub konkretne wydarzenie, kiedy klauzula zostaje zniesiona, chyba że mają uzasadnione powody, aby tego nie robić.

16. SGR przeprowadza regularne przeglądy informacji niejawnych UE znajdujących się w jego posiadaniu, by stwierdzić, czy dana klauzula tajności ma nadal zastosowanie. SGR tworzy system służący do przeglądu klauzul tajności nadanych zarejestrowanym informacjom niejawnym UE, których jest wytwórcą, nie rzadziej niż co pięć lat. Taki przegląd nie jest konieczny, jeżeli wytwórca wskazał na samym początku, że klauzula nadana danym informacjom zostanie automatycznie obniżona lub zniesiona, a informacje te zostały odpowiednio oznaczone.

III. REJESTRACJA INFORMACJI NIEJAWNYCH UE DO CELÓW BEZPIECZEŃSTWA

Przepisy ogólne

17. Do celów niniejszej decyzji rejestracja do celów bezpieczeństwa (zwana dalej „rejestracją”) oznacza stosowanie procedur umożliwiających zidentyfikowanie w każdej chwili posiadacza dokumentu niejawnego oraz zarejestrowanie etapów istnienia tego dokumentu, w tym jego zniszczenia.

18. Rejestrowane są wszystkie dokumenty o klauzuli CONFIDENTIEL UE i wyższej lub o klauzulach stanowiących ich odpowiedniki. Dokumenty takie są rejestrowane przez kancelarię tajną, która jest odpowiedzialna za rejestrację w danej jednostce organizacyjnej, każdorazowo w momencie ich wpłynięcia do jednostki organizacyjnej lub wysłania z tej jednostki. W przypadku CIS procedury rejestracji mogą być stosowane w ramach działań samego CIS.

19. Zarejestrowane dokumenty niejawne podlegają w miarę możliwości wymianie między kancelariami tajnymi. Dokumenty te są dostarczane odbiorcy przez odpowiedzialną za nie kancelarię tajną.

20. Fakt rejestracji zapisywany jest w rejestrze lub przy użyciu elektronicznego narzędzia rejestracji. Zarejestrowane informacje stanowią niezbędne minimum służące wyłącznie do zidentyfikowania danego dokumentu, takie jak numer referencyjny, temat, data, a w stosownych przypadkach numer kopii.

21. Osoba posiadająca zarejestrowany dokument niejawny potwierdza jego posiadanie przez podpisanie pokwitowania. Pokwitowanie zawiera zasadniczo tylko informacje jawne, takie jak numer referencyjny dokumentu, numer rejestracji, datę, a w stosownych przypadkach numer kopii dokumentu.

22. Informacje niejawne wymieniane z państwem trzecim lub organizacją międzynarodową są rejestrowane w osobnych rejestrach tworzonych dla poszczególnych stron trzecich. Rejestry są oddzielone od pozostałych informacji na temat rejestracji. W kancelariach tajnych rejestry przechowuje się w taki sposób, aby informacje niejawne pochodzące od różnych stron trzecich były rozdzielone.

23. Główna kancelaria tajna w SGR prowadzi rejestr wszystkich informacji niejawnych udostępnionych przez Radę i SGR państwom trzecim i organizacjom międzynarodowym i wszystkich informacji niejawnych otrzymanych od tych państw i organizacji.

24. Rada zatwierdza politykę bezpieczeństwa dotyczącą rejestrowania informacji niejawnych UE do celów bezpieczeństwa.

System kancelarii tajnych

25. Dla każdej jednostki organizacyjnej w SGR i w administracji krajowej państw członkowskich, w których odbywa się praca z wykorzystaniem informacji niejawnych UE, określa się odpowiedzialną kancelarię tajną. Kancelarie tajne dbają o to, by praca z wykorzystaniem informacji niejawnych UE, co do których istnieje obowiązek rejestracji, odbywała się w jednostkach organizacyjnych zgodnie z niniejszą decyzją.

26. Kancelarie tajne otrzymują, rejestrują, kopiują, dystrybuują, przechowują i niszczą informacje niejawne o klauzuli CONFIDENTIEL UE i wyższej. Zadania te mogą być wykonywane w ramach jednej kancelarii tajnej lub przez powołanie oddzielnych kancelarii tajnych. Jeśli jest to konieczne ze względów organizacyjnych, powoływane są podległe kancelarie tajne będące częściami danej kancelarii tajnej.

27. Kancelarie tajne uznaje się za strefy zabezpieczone określone w załączniku II.

28. Osoba zarządzająca kancelarią tajną ds. informacji niejawnych UE jest odpowiedzialna za:

    (a) przechowywanie aktualnego wykazu wszystkich kancelarii tajnych, z którymi zwykle wymienia informacje niejawne;

    (b) przechowywanie aktualnego wykazu wszystkich sprawdzonych pod względem bezpieczeństwa osób w jednostkach organizacyjnych, wobec których kancelaria tajna ma obowiązki rejestracyjne;

    (c) dopilnowanie, by kancelaria tajna regularnie przeprowadzała szczegółową inwentaryzację wszystkich informacji niejawnych UE, za które jest odpowiedzialna. Uważa się, że kancelaria jest odpowiedzialna za dokument, jeśli fizycznie go posiada, posiada zaświadczenie od odbiorcy, do którego dokument ten został przekazany, posiada certyfikat zniszczenia tego dokumentu lub posiada instrukcję o obniżeniu lub zniesieniu klauzuli tajności tego dokumentu;

    (d) przechowywanie wykazu podległych jej kancelarii tajnych;

(e) dopilnowanie, by podległe kancelarie tajne przesyłały wyniki wszelkich inwentaryzacji kancelarii tajnej, której podlegają, w terminie wyznaczonym przez tę kancelarię tajną;

Kancelarie tajne ds. informacji o klauzuli TRES SECRET UE

29. W państwach członkowskich i w SGR wyznacza się kancelarię tajną będącą głównym organem otrzymującym i przesyłającym informacje niejawne o klauzuli TRES SECRET UE. W razie konieczności można wyznaczyć podległe kancelarie tajne do pracy z wykorzystaniem takich informacji do celów rejestracji. Podlegają one głównej kancelarii tajnej ds. informacji o klauzuli TRES SECRET UE.

30. Takie podległe kancelarie tajne nie mogą przekazywać dokumentów o klauzuli TRES SECRET UE bezpośrednio innym podległym kancelariom podlegającym tej samej głównej kancelarii tajnej ds. informacji o klauzuli TRES SECRET UE bez wyraźnego upoważnienia z jej strony. Każda wymiana dokumentów o tej klauzuli pomiędzy dwiema podległymi kancelariami niepodlegającymi tej samej głównej kancelarii tajnej ds. informacji o klauzuli TRES SECRET UE odbywa się za pośrednictwem głównych kancelarii tajnych ds. informacji o klauzuli TRES SECRET UE.

VIII. KOPIOWANIE I TŁUMACZENIE DOKUMENTÓW NIEJAWNYCH UE

31. Do kopiowania lub tłumaczenia dokumentów o klauzuli TRES SECRET UE potrzebna jest wcześniejsza pisemna zgoda ich wytwórcy.

32. Jeżeli wytwórca dokumentów o klauzuli SECRET UE i niższej nie zgłosił zastrzeżeń co do ich kopiowania lub tłumaczenia, dokumenty takie można kopiować lub tłumaczyć na zlecenie posiadacza.

33. Kopie zarejestrowanych dokumentów niejawnych mogą być przygotowywane i dystrybuowane wyłącznie przez odpowiedzialną kancelarię tajną.

34. Środki bezpieczeństwa, które odnoszą się do oryginału dokumentu, mają zastosowanie do jego kopii i tłumaczeń.

V. FIZYCZNE PRZEWOŻENIE INFORMACJI NIEJAWNYCH UE

35. Fizyczne przewożenie informacji niejawnych podlega środkom ochronnym określonym w pkt 37–49 poniżej. Gdy informacje niejawne UE są przewożone z użyciem środków elektronicznych, niezależnie od przepisów art. 10 ust. 4, poniższe środki ochronne mogą być uzupełnione odpowiednimi technicznymi środkami zaradczymi zgodnie z wytycznymi właściwej władzy bezpieczeństwa, tak aby zminimalizować ryzyko utraty lub narażenia na szwank bezpieczeństwa informacji.

36. Właściwe władze bezpieczeństwa w SGR i w państwach członkowskich wydają instrukcje dotyczące przewożenia informacji niejawnych UE zgodnie z przepisami niniejszej decyzji.

W obrębie jednego budynku lub grupy budynków stanowiącej zamkniętą całość

37. Informacje niejawne UE przewożone w ramach budynku lub grupy budynków stanowiącej zamkniętą całość są zakrywane, aby nie można było zobaczyć ich treści.

38. W ramach budynku lub grupy budynków stanowiącej zamkniętą całość informacje o klauzuli TRES SECRET UE są przewożone w zabezpieczonej kopercie, na której znajduje się jedynie nazwisko adresata.

W obrębie państwa członkowskiego

Opakowanie

39. Informacje o klauzuli CONFIDENTIEL UE i wyższej przewożone między budynkami lub obiektami w jednym państwie członkowskim są opakowane w taki sposób, by chronić je przed ujawnieniem nieuprawnionym osobom. Zastosowanie mają następujące zasady:

(a) informacje są zamknięte w dwóch mocnych nieprzezroczystych kopertach;

(b) wewnętrzna koperta jest zamknięta, opatrzona właściwym oznaczeniem dokumentu towarzyszącym klauzuli oraz wszelkimi dodatkowymi oznaczeniami, a także pełną nazwą i adresem odbiorcy;

(c) koperta zewnętrzna opatrzona jest nazwą i adresem odbiorcy;

(d) na kopercie zewnętrznej nie umieszcza się informacji o klauzuli znajdujących się wewnątrz dokumentów ani o tym, że koperta zawiera informacje niejawne UE;

(e) jeżeli informacje niejawne UE są przewożone za pośrednictwem służb kurierskich, na kopercie zewnętrznej znajduje się wyraźny napis: „wyłącznie za pośrednictwem służb kurierskich".

40. Informacje oznaczone klauzulą RESTREINT UE przewozi się co najmniej w jednej nieprzezroczystej kopercie. Na kopercie brak jest oznaczeń wskazujących, że zawiera ona informacje niejawne UE.

Przewożenie

41. Fizyczny przewóz informacji o klauzuli SECRET UE między budynkami lub obiektami w obrębie jednego państwa członkowskiego odbywa się następująco:

(a) za pośrednictwem wojskowych lub rządowych służb kurierskich;

(b) za pośrednictwem krajowych usług pocztowych lub prywatnych służb kurierskich, zgodnie z krajowymi przepisami ustawowymi i wykonawczymi;

(c) osobiście, pod warunkiem że:

(i) w przypadku rejestrowanych informacji niejawnych UE fakt ten jest udokumentowany w odpowiednich rejestrach;

(ii) informacje niejawne UE przez cały czas znajdują się w posiadaniu osoby je przewożącej, chyba że są przechowywane zgodnie z wymogami określonymi w załączniku II;

(iii) informacje niejawne UE nie są po drodze otwierane ani czytane w miejscach publicznych;

(iv) odnośne osoby informuje się o ich obowiązkach w zakresie bezpieczeństwa;

(v) w odpowiednich przypadkach odnośnym osobom wydaje się list kurierski.

42. Fizyczny przewóz informacji o klauzuli TRES SECRET UE między budynkami lub obiektami w jednym państwie członkowskim odbywa się zgodnie z pkt 41 ppkt a).

Z jednego państwa członkowskiego do drugiego

43. Informacje niejawne UE przewożone z jednego państwa członkowskiego do drugiego są opakowane zgodnie z pkt 39 i 40.

44. Fizyczny przewóz informacji o klauzuli SECRET UE z jednego państwa członkowskiego do drugiego odbywa się następująco:

(a) za pośrednictwem wojskowych lub dyplomatycznych służb kurierskich;

(b) za pośrednictwem krajowych usług pocztowych lub prywatnych służb kurierskich, zgodnie z krajowymi przepisami ustawowymi i wykonawczymi;

(c) osobiście, pod warunkiem że:

(i) w przypadku rejestrowanych informacji niejawnych UE fakt ten jest udokumentowany w odpowiednich rejestrach;

(ii) informacje niejawne UE przez cały czas znajdują się w posiadaniu osoby je przewożącej, chyba że są przechowywane zgodnie z wymogami określonymi w załączniku II;

(iii) informacje niejawne UE nie są po drodze otwierane ani czytane w miejscach publicznych;

(iv) odnośne osoby informuje się o ich obowiązkach w zakresie bezpieczeństwa;

(v) odnośna osoba posiada list kurierski zawierający informacje o paczce i upoważniający ją do przewożenia tej paczki.

45. Fizyczny przewóz informacji niejawnych o klauzuli TRES SECRET UE z jednego państwa członkowskiego do drugiego następuje zgodnie z pkt 44 ppkt a).

Z terytorium UE do państwa trzeciego

46. Informacje niejawne UE przewożone z terytorium UE do państwa trzeciego są opakowane zgodnie z pkt 39 i 40.

47. Fizyczny przewóz informacji o klauzuli SECRET UE z terytorium UE do państwa trzeciego odbywa się następująco:

(a) za pośrednictwem wojskowych lub dyplomatycznych służb kurierskich;

(b) osobiście, pod warunkiem że:

(i) na paczce znajduje się urzędowa pieczęć lub sposób zapakowania wskazuje na to, że jest to przesyłka urzędowa i nie powinna podlegać kontroli celnej ani kontroli bezpieczeństwa;

(ii) odnośna osoba posiada list kurierski zawierający informacje o paczce i upoważniający ją do przewożenia tej paczki.

48. Informacje o klauzuli RESTREINT UE mogą być przewożone także za pośrednictwem krajowych usług pocztowych lub prywatnych służb kurierskich.

49. Fizyczny przewóz informacji niejawnych o klauzuli TRES SECRET UE z terytorium UE do państwa trzeciego następuje zgodnie z pkt 47 ppkt a).

VI. NISZCZENIE DOKUMENTÓW NIEJAWNYCH UE

50. Dokumenty niejawne UE, które nie są już potrzebne, mogą zostać zniszczone bez uszczerbku dla odpowiednich przepisów ustawowych i wykonawczych dotyczących archiwizowania.

51. Dokumenty podlegające rejestracji zgodnie z art. 10 ust. 2 są niszczone przez odpowiedzialną kancelarię tajną na polecenie posiadacza lub właściwego organu. Rejestry i inne informacje dotyczące rejestracji są odpowiednio uaktualniane.

52. W odniesieniu do dokumentów niejawnych o klauzuli SECRET UE lub TRES SECRET UE niszczenie przebiega w obecności świadków, którzy zostali sprawdzeni pod względem bezpieczeństwa co najmniej do poziomu klauzuli niszczonego dokumentu.

53. Osoba dokonująca rejestracji, a w stosownym przypadku także świadek podpisują certyfikat zniszczenia, który zostaje umieszczony w dokumentacji kancelarii tajnej. Protokoły zniszczenia dokumentów o klauzuli TRES SECRET UE przechowuje się w kancelarii tajnej przez okres dziesięciu lat, a dokumentów o klauzuli CONFIDENTIEL UE i SECRET UE – przez okres trzech lat.

54. Dokumenty niejawne, w tym dokumenty o klauzuli RESTREINT UE, są niszczone przy zastosowaniu metod, które spełniają odpowiednią europejską normę lub normy równoważne lub są zatwierdzone przez państwa członkowskie zgodnie z krajowymi technicznymi normami, tak by nie mogły zostać całkowicie lub częściowo odtworzone.

VII. KONTROLE I WIZYTY OCENIAJĄCE

55. Użycie terminu „kontrola” oznacza poniżej każdą

- kontrolę zgodnie z art. 10 ust. 3, art. 15 ust. 2 lit. e), f) oraz g); lub

- wizytę oceniającą zgodnie z art. 12 ust. 5,

służącą ocenie skuteczności środków wdrożonych, aby chronić informacje niejawne UE.

56. Kontrole przeprowadza się m.in., aby:

(a) dopilnować przestrzegania określonych w niniejszej decyzji wymaganych norm minimalnych w zakresie ochrony informacji niejawnych UE;

(b) podkreślić znaczenie bezpieczeństwa i skutecznej kontroli ryzyka wewnątrz kontrolowanych podmiotów;

(c) zalecić środki zaradcze mające złagodzić konkretne skutki, jakie może powodować utrata poufności, integralności lub dostępności informacji niejawnych; oraz

(d) ulepszyć istniejące programy, opracowane przez władze bezpieczeństwa, dotyczące szkoleń i upowszechniania wiedzy w dziedzinie bezpieczeństwa.

57. Przed końcem każdego roku kalendarzowego Rada przyjmuje na następny rok program kontroli przewidziany w art. 15 ust. 1 lit. c). Konkretne daty każdej kontroli są określane w porozumieniu z daną agencją lub organem UE, państwem członkowskim, państwem trzecim lub organizacją międzynarodową.

Prowadzenie kontroli

58. Kontrole przeprowadzane są, aby sprawdzić odnośne zasady, przepisy i procedury stosowane przez kontrolowany podmiot oraz stwierdzić, czy praktyki w nim stosowane odpowiadają minimalnym normom określonym w niniejszej decyzji i przepisom dotyczącym wymiany informacji niejawnych z tym podmiotem.

59. Kontrole są przeprowadzane w dwóch etapach. Przed samą kontrolą w razie potrzeby organizowane jest posiedzenie przygotowawcze z odnośnym podmiotem. Po spotkaniu przygotowawczym zespół kontrolny ustala, w porozumieniu z wymienionym podmiotem, szczegółowy program kontroli obejmujący wszystkie obszary bezpieczeństwa. Zespół kontrolny ma dostęp do wszystkich miejsc, w których odbywa się praca z wykorzystaniem informacji niejawnych UE, w szczególności do kancelarii tajnych i punktów objętych CIS.

60. Odpowiedzialność za prowadzenie kontroli w krajowych administracjach państw członkowskich oraz w państwach trzecich i organizacjach międzynarodowych ponosi wspólny zespół kontrolny SGR i Komisji Europejskiej w pełni współpracujący z urzędnikami kontrolowanego jednostki.

61. Kontrole agencji lub organów UE prowadzone są przez Biuro ds. Bezpieczeństwa SGR przy wsparciu ekspertów władz bezpieczeństwa kraju, w którym znajduje się agencja lub organ. W kontroli może brać udział dyrekcja ds. bezpieczeństwa Komisji Europejskiej, jeżeli prowadzi regularną wymianę informacji niejawnych UE z daną agencją lub organem.

62. Komitet ds. Bezpieczeństwa dokonuje szczegółowych ustaleń co do wsparcia ze strony ekspertów NSA podczas kontroli w agencjach i organach UE oraz państwach trzecich i organizacjach międzynarodowych.

Sprawozdania z kontroli

63. Pod koniec kontroli kontrolowanemu podmiotowi przedstawiane są główne wnioski i zalecenia. Następnie pod nadzorem władzy bezpieczeństwa SGR (Biuro ds. Bezpieczeństwa) sporządzane jest sprawozdanie z kontroli. W przypadku gdy zostały zaproponowane działanie naprawcze i zalecenia, w sprawozdaniu należy zamieścić odpowiednio szczegółowe dane uzasadniające dojście do takich wniosków. Sprawozdanie przekazywane jest właściwym organom kontrolowanego podmiotu.

64. W przypadku kontroli przeprowadzanych w krajowych administracjach państw członkowskich:

(a) projekt sprawozdania z kontroli zostanie przekazany odnośnej NSA w celu sprawdzenia, czy jest on poprawny pod względem merytorycznym i czy nie zawiera informacji oznaczonych klauzulą wyższą niż RESTREINT UE;

o ile NSA danego państwa członkowskiego nie wystąpią o wstrzymanie ogólnej dystrybucji, sprawozdania z kontroli przekazywane są członkom Komitetu ds. Bezpieczeństwa oraz dyrekcji ds. bezpieczeństwa Komisji Europejskiej; sprawozdanie otrzymuje klauzulę RESTREINT UE;

Pod nadzorem władzy bezpieczeństwa SGR (Biuro ds. Bezpieczeństwa) przygotowywane jest okresowe sprawozdanie mające na celu uwypuklenie doświadczeń nabytych w wyniku kontroli w państwach członkowskich w danym okresie.

65. W przypadku wizyt oceniających w państwach trzecich i organizacjach międzynarodowych sprawozdanie przekazywane jest członkom Komitetu ds. Bezpieczeństwa oraz dyrekcji ds. bezpieczeństwa Komisji Europejskiej. Sprawozdanie opatrzone jest co najmniej klauzulą RESTREINT UE. Wszystkie działania naprawcze są weryfikowane podczas następnej wizyty, a sprawozdanie na ich temat przekazywane jest Komitetowi ds. Bezpieczeństwa.

66. W przypadku kontroli w agencjach i organach UE sprawozdanie z kontroli przekazywane jest członkom Komitetu ds. Bezpieczeństwa oraz dyrekcji ds. bezpieczeństwa Komisji Europejskiej. Projekt sprawozdania z kontroli przekazywany jest odnośnej agencji lub organu w celu sprawdzenia, czy jest on zgodny z faktami i czy nie zawiera informacji oznaczonych klauzulą wyższą niż RESTREINT UE. Wszystkie działania naprawcze są weryfikowane podczas następnej wizyty, a sprawozdanie na ich temat przekazywane jest Komitetowi ds. Bezpieczeństwa.

67. Władza bezpieczeństwa SGR przeprowadza regularne kontrole jednostek organizacyjnych w SGR w celach przedstawionych w pkt 56.

Lista kontrolna

68. Władza bezpieczeństwa SGR (Biuro ds. Bezpieczeństwa) sporządza i uaktualnia listę kontrolną wykorzystywaną podczas kontroli bezpieczeństwa i zawierającą kwestie, które należy sprawdzić w trakcie inspekcji. Lista kontrolna przekazywana jest Komitetowi ds. Bezpieczeństwa.

69. Informacji niezbędnych do uzupełnienia listy kontrolnej udziela, w szczególności podczas kontroli, personel zajmujący się kontrolą bezpieczeństwa w jednostce, w której przeprowadzana jest kontrola. Po wypełnieniu listy kontrolnej szczegółowymi odpowiedziami opatruje się ją klauzulą tajności w porozumieniu z kontrolowaną jednostką. Lista ta nie jest częścią sprawozdania z kontroli.

BEZPIECZEŃSTWO PRZEMYSŁOWE

I. WPROWADZENIE

1. Niniejszy załącznik zawiera przepisy dotyczące wprowadzania w życie art. 11. Ustanawia on ogólne przepisy w zakresie bezpieczeństwa mające zastosowanie do podmiotów prowadzących działalność przemysłową lub inną podczas negocjacji poprzedzających zawarcie umowy oraz na wszystkich etapach istnienia umów niejawnych zawartych przez SGR.

2. Rada zatwierdza politykę bezpieczeństwa przemysłowego, w szczególności szczegółowe wymogi w odniesieniu do FSC, dokumentu określającego aspekty bezpieczeństwa (zwanego dalej „SAL"), wizyt, przekazywania i przewożenia informacji niejawnych UE.

II. ELEMENTY DOTYCZĄCE BEZPIECZEŃSTWA W UMOWIE NIEJAWNEJ

Przewodnik nadawania klauzul (SCG)

3. Przed ogłoszeniem zaproszenia do składania ofert lub zawarciem umowy niejawnej SGR, jako instytucja zamawiająca, określa klauzulę tajności wszelkich informacji, które należy dostarczyć oferentom i wykonawcom, jak również klauzulę tajności wszelkich informacji, które mają być wytworzone przez wykonawcę. W tym celu SGR opracowuje SCG, który należy stosować podczas wykonywania umów.

4. Do określania klauzuli tajności różnych elementów umowy niejawnej zastosowanie mają następujące zasady:

(a) podczas opracowywania SCG, SGR uwzględnia wszystkie odpowiednie aspekty bezpieczeństwa, w tym klauzulę nadaną informacjom, które ich wytwórca przekazał i których wykorzystanie zatwierdził do celów umowy;

(b) ogólna klauzula tajności umowy nie może być niższa od najwyższej klauzuli tajności wśród jej elementów; oraz

(c) w odpowiednich przypadkach SGR działa w porozumieniu z NSA/DSA lub jakimikolwiek innymi zainteresowanymi władzami bezpieczeństwa na wypadek jakichkolwiek zmian klauzul tajności informacji wytworzonych przez wykonawców lub przekazanych im podczas wykonywania umowy oraz wprowadzania wszelkich odnośnych zmian do SCG.

Dokument określający aspekty bezpieczeństwa (SAL)

5. Wymogi bezpieczeństwa dotyczące poszczególnych umów opisane są w SAL. SAL w odpowiednich przypadkach zawiera SCG i stanowi integralną część niejawnej umowy o wykonawstwo lub podwykonawstwo.

6. SAL zawiera przepisy zobowiązujące wykonawcę lub podwykonawcę do przestrzegania minimalnych norm przedstawionych w niniejszej decyzji. Nieprzestrzeganie tych minimalnych norm może spowodować rozwiązanie umowy.

Instrukcje bezpieczeństwa programu/projektu (PSI)

7. W zależności od zakresu programów lub projektów obejmujących dostęp do informacji niejawnych UE, pracę z ich wykorzystaniem lub ich przechowywanie, organ wyznaczony do zarządzania danym programem lub projektem może sporządzić specjalne instrukcje bezpieczeństwa programu/projektu (zwane dalej „PSI”). PSI wymagają zatwierdzenia przez NSA/DSA państw członkowskich lub jakakolwiek inna właściwa władza bezpieczeństwa uczestnicząca w programie/projekcie i mogą zawierać dodatkowe wymogi bezpieczeństwa.

III. ŚWIADECTWO BEZPIECZEŃSTWA PRZEMYSŁOWEGO (FSC)

8. FSC przyznawane jest przez NSA lub DSA, lub jakiekolwiek inne właściwe władze bezpieczeństwa państwa członkowskiego w celu zaświadczenia zgodnie z krajowymi przepisami ustawowymi i wykonawczymi, że dany podmiot prowadzący działalność przemysłową lub inną jest w stanie zapewnić w swoich obiektach ochronę informacji niejawnych UE odpowiednią do określonego poziomu klauzuli. Świadectwo to przedstawiane jest SGR, będącemu instytucją zamawiającą, przed dostarczeniem informacji niejawnych UE wykonawcy, podwykonawcy, potencjalnemu wykonawcy lub potencjalnemu podwykonawcy, lub umożliwieniem im dostępu do takich informacji.

9. Przy wydawaniu FSC odpowiednie NSA lub DSA sprawdzają przynajmniej, czy:

   a) podmiot prowadzący działalność przemysłową lub inną stworzył w obiekcie system bezpieczeństwa, który obejmuje wszystkie odpowiednie środki bezpieczeństwa niezbędne do ochrony informacji lub materiałów niejawnych o klauzuli CONFIDENTIEL UE lub wyższej zgodnie z minimalnymi normami niniejszej decyzji;

   b) status bezpieczeństwa osobowego kadry zarządzającej, właścicieli i pracowników, którzy mają mieć dostęp do informacji niejawnych o klauzuli CONFIDENTIEL UE lub wyższej, został ustalony zgodnie z wymogami określonymi w załączniku I do niniejszej decyzji;

   c) podmiot prowadzący działalność przemysłową lub inną powołał urzędnika ds. bezpieczeństwa obiektów, który jest odpowiedzialny wobec kierownictwa za egzekwowanie obowiązków dotyczących bezpieczeństwa w obrębie tego podmiotu.

10. Wycofanie FSC przez odnośne NSA/DSA lub jakakolwiek inna właściwa władza bezpieczeństwa upoważnia SGR, jako instytucję zamawiającą, do rozwiązania umowy niejawnej lub wykluczenia oferenta z postępowania.

11. W stosownych przypadkach SGR powiadamia – jako instytucja zamawiająca – odpowiednie NSA/DSA lub jakiekolwiek inne właściwe władze bezpieczeństwa o tym, że FSC jest wymagane na etapie poprzedzającym zawarcie umowy lub do wykonywania umowy.

12. Instytucja zamawiająca nie zawiera umowy niejawnej z wybranym oferentem, zanim nie otrzyma potwierdzenia od NSA/DSA lub jakiejkolwiek innej właściwej władzy bezpieczeństwa państwa członkowskiego, w którym zarejestrowany jest ten wykonawca lub podwykonawca, że w zależności od wymogu wydane zostało właściwe FSC.

13. NSA/DSA lub jakakolwiek inna właściwa władza bezpieczeństwa, który wydał FSC, powiadamiają instytucję zamawiającą o wszelkich zmianach dotyczących FSC.

IV. NIEJAWNE UMOWY O WYKONAWSTWO I PODWYKONAWSTWO

14. Jeżeli informacje niejawne UE przekazywane są oferentowi na etapie poprzedzającym zawarcie umowy, zaproszenie do złożenia oferty zawiera przepis zobowiązujący oferenta, który nie przedłoży oferty lub który nie zostanie wybrany, do zwrotu wszystkich dokumentów niejawnych w określonym terminie.

15. Po przyznaniu niejawnej umowy o wykonawstwo lub podwykonawstwo SGR, jako instytucja zamawiająca, powiadamia NSA/DSA lub jakakolwiek inna właściwa władza bezpieczeństwa wykonawcy lub podwykonawcy o zawartych w tej umowie przepisach bezpieczeństwa.

16. W przypadku rozwiązania takich umów SGR, jako instytucja zamawiająca, lub, w stosownym przypadku, NSA/DSA lub jakakolwiek inna właściwa władza bezpieczeństwa niezwłocznie powiadamiają o tym fakcie NSA/DSA lub jakąkolwiek inną właściwą władzę bezpieczeństwa państwa członkowskiego, w którym zarejestrowany jest wykonawca lub podwykonawca.

17. Z reguły od wykonawcy lub podwykonawcy wymaga się zwrotu do instytucji zamawiającej wszelkich posiadanych przez niego informacji niejawnych UE po rozwiązaniu niejawnej umowy o wykonawstwo lub podwykonawstwo.

18. W SAL określa się przepisy szczegółowe dotyczące niszczenia informacji niejawnych UE podczas wykonywania umowy lub po jej rozwiązaniu.

19. Jeżeli wykonawca lub podwykonawca są upoważnieni do zachowania informacji niejawnych UE po rozwiązaniu umowy, nadal spełniane są minimalne normy zawarte w niniejszej decyzji i wykonawca lub podwykonawca nadal chronią poufność informacji niejawnych UE.

20. Przed zleceniem podwykonawstwa części umowy niejawnej wykonawca uzyskuje zgodę SGR jako instytucji zamawiającej. Wykonawca odpowiada za dopilnowanie, by wszystkie czynności podwykonawcze były podejmowane zgodnie z minimalnymi normami określonymi w niniejszej decyzji i nie dostarcza informacji niejawnych UE podwykonawcy bez uprzedniej pisemnej zgody instytucji zamawiającej.

21. Warunki, na których wykonawca może zlecić podwykonawstwo, są określone w ofercie oraz w umowie. Nie można zawrzeć żadnej umowy podwykonawczej z podmiotami prowadzącymi działalność przemysłową lub inną zarejestrowanymi w państwie niebędącym członkiem UE bez uprzedniego pisemnego upoważnienia ze strony SGR jako instytucji zamawiającej.

22. W odniesieniu do informacji niejawnych UE wytworzonych lub wykorzystywanych do pracy przez wykonawcę lub podwykonawcę prawa przysługujące na wytwórcy są wykonywane przez instytucję zamawiającą.

V. WIZYTY W ZWIĄZKU Z UMOWAMI NIEJAWNYMI

23. NSA/DSA państw członkowskich, SGR i wykonawcy wspólnie ustalają wizyty w swoich obiektach pracowników lub przedstawicieli uczestniczących w działalności przemysłowej lub innej wymagającej dostępu do informacji o klauzuli tajności CONFIDENTIEL UE i SECRET UE lub w przypadku konieczności dostępu do stref zabezpieczonych.

24. Wizyty przeprowadzane w ramach takich umów są ustalane z NSA/DSA lub jakimkolwiek inną zainteresowaną właściwą władzą bezpieczeństwa. NSA/DSA lub jakakolwiek inna właściwa władza bezpieczeństwa mogą jednak uzgodnić procedurę umożliwiającą bezpośrednie ustalanie wizyt pracowników podmiotu prowadzącego działalność przemysłową lub inną.

25. Wszystkie osoby wizytujące posiadają odpowiednie PBO i podlegają zasadzie ograniczonego dostępu, co uprawnia je do dostępu do informacji niejawnych UE związanych z umową zawartą przez SGR.

26. Osobom wizytującym umożliwia się dostęp wyłącznie do informacji niejawnych UE związanych z celem wizyty.

IX. PRZEKAZYWANIE I PRZEWOŻENIE INFORMACJI NIEJAWNYCH UE

27. Do elektronicznego przekazywania informacji niejawnych UE zastosowanie mają odnośne przepisy art. 9 i załącznika III do niniejszej decyzji

28. Do fizycznego przewożenia informacji niejawnych UE zastosowanie mają odnośne przepisy załącznika IV do niniejszej decyzji zgodnie z krajowymi przepisami ustawowymi i wykonawczymi.

29. Do określania zabezpieczeń obowiązujących podczas fizycznego przewożenia informacji niejawnych UE mają zastosowanie następujące zasady:

    (a) bezpieczeństwo zapewnia się na wszystkich etapach przewozu oraz we wszelkich okolicznościach, począwszy od miejsca wyjazdu do ostatecznego miejsca przeznaczenia;

    (b) stopień ochrony przysługujący przesyłce zależy od najwyższej klauzuli tajności materiału, który zawiera przesyłka;

    (c) firmy dokonujące przewozu w stosownych przypadkach uzyskują FSC. W takich przypadkach pracownicy zajmujący się przesyłką są odpowiednio sprawdzani pod względem bezpieczeństwa zgodnie z niniejszym załącznikiem;

(d) przed jakimkolwiek transgranicznym przemieszczeniem materiałów, którym nadano klauzulę CONFIDENTIEL UE lub SECRET UE, nadawca sporządza plan przewozu, który jest zatwierdzany przez odnośne NSA/DSA lub jakakolwiek inna zainteresowana właściwa władza bezpieczeństwa;

(e) przejazdy odbywają się w miarę możliwości bezpośrednio między dwoma punktami i kończą się tak szybko, jak pozwolą na to okoliczności;

(f) jeżeli jest to możliwe, trasy przebiegają wyłącznie przez terytoria państw członkowskich. Podróż trasami przebiegającymi przez terytoria państw innych niż państwa członkowskie UE powinna się odbywać wyłącznie pod warunkiem zatwierdzenia przez NSA/DSA lub jakakolwiek inna właściwa władza bezpieczeństwa zarówno państwa nadawcy, jak i państwa odbiorcy.

VII. PRZEKAZYWANIE INFORMACJI NIEJAWNYCH UE WYKONAWCOM ZNAJDUJĄCYM SIĘ W PAŃSTWACH TRZECICH

30. Informacje niejawne UE są przekazywane wykonawcom i podwykonawcom znajdującym się w państwach trzecich zgodnie ze środkami bezpieczeństwa uzgodnionymi przez SGR, jako instytucję zamawiającą, z NSA/DSA państwa trzeciego, w którym zarejestrowany jest wykonawca.

VIII. PRACA Z WYKORZYSTANIEM INFORMACJI NIEJAWNYCH O KLAUZULI RESTREINT UE ORAZ PRZECHOWYWANIE TAKICH INFORMACJI

31. W porozumieniu z NSA/DSA państwa członkowskiego SGR, jako instytucja zamawiająca, jest upoważniony na podstawie przepisów umownych do przeprowadzania wizyt w obiektach wykonawców/podwykonawców, aby sprawdzić, czy spełnione są odpowiednie środki bezpieczeństwa mające zapewnić ochronę informacji niejawnych UE oznaczonych klauzulą RESTREINT UE zgodnie z wymogami umowy.

32. W zakresie, jaki jest wymagany na mocy krajowych przepisów ustawowych i wykonawczych, NSA/DSA lub jakiekolwiek inne właściwe władze bezpieczeństwa są powiadamiane o umowach zawierających informacje niejawne o klauzuli RESTREINT UE.

33. W przypadku umów zawierających informacje o klauzuli RESTREINT UE od wykonawców, podwykonawców ani ich personelu nie wymaga się posiadania FSC ani PBO, chyba że wymagają tego krajowe przepisy ustawowe i wykonawcze państw członkowskich.

34. Jako instytucja zamawiająca, SGR analizuje odpowiedzi na zaproszenia do składania ofert w przypadku umów, które wymagają dostępu do informacji o klauzuli RESTREINT UE, niezależnie od jakichkolwiek wymogów związanych z FSC lub PBO nakładanych przez krajowe przepisy ustawowe i wykonawcze.

35. Warunki, na których wykonawca może zlecić podwykonawstwo, są zgodne z pkt 20.

36. Jeżeli umowa obejmuje przetwarzanie informacji niejawnych UE o klauzuli RESTREINT UE przez CIS, który eksploatuje wykonawca, SGR jako instytucja zamawiająca lub inne właściwe organy dopilnowują, aby umowa określała niezbędne wymogi techniczne i administracyjne dotyczące akredytacji CIS, które są proporcjonalne do szacowanego ryzyka z uwzględnieniem wszystkich odpowiednich czynników.

ZAŁĄCZNIK VI

WYMIANA INFORMACJI NIEJAWNYCH Z PAŃSTWAMI TRZECIMI I ORGANIZACJAMI MIĘDZYNARODOWYMI

I. WPROWADZENIE

1. Niniejszy załącznik zawiera przepisy dotyczące wprowadzania w życie art. 12.

II. RAMY REGULUJĄCE WYMIANĘ INFORMACJI NIEJAWNYCH

2. W przypadku gdy Rada stwierdza, że istnieje długoterminowa potrzeba wymiany informacji niejawnych:

   - zawarta zostaje umowa o bezpieczeństwie informacji lub

   - zawarte zostaje porozumienie administracyjne,

   zgodnie z art. 12 ust. 2 i sekcjami III i IV poniżej oraz na podstawie zalecenia Komitetu ds. Bezpieczeństwa.

3. Jeżeli informacje niejawne UE wytworzone do celów operacji EPBiO mają zostać przekazane państwom trzecim lub organizacjom międzynarodowym uczestniczącym w takiej operacji, a nie istnieją żadne z ram, o których mowa w pkt 2, wymiana informacji niejawnych UE z uczestniczącym w operacji państwem trzecim lub organizacją międzynarodową regulowana jest na mocy:

   - umowy ramowej w sprawie udziału; lub

   - umowy *ad hoc* w sprawie udziału; lub

   - jeżeli nie zawarto żadnej z powyższych umów – porozumienia administracyjnego *ad hoc*.

4. Jeżeli brak jest ram, o których mowa w pkt 2 i 3, a podjęta zostaje decyzja o udostępnieniu informacji niejawnych UE państwu trzeciemu lub organizacji międzynarodowej w wyjątkowym trybie *ad hoc* zgodnie z sekcją VI poniżej, od tego państwa trzeciego lub organizacji międzynarodowej należy uzyskać pisemną gwarancję, że chronią one wszelkie ujawnione im informacje niejawne UE zgodnie z podstawowymi zasadami i minimalnymi normami bezpieczeństwa przedstawionymi w niniejszej decyzji.

III. UMOWY O BEZPIECZEŃSTWIE INFORMACJI

5. Umowy o bezpieczeństwie informacji określają podstawowe zasady i minimalne normy mające zastosowanie do wymiany informacji niejawnych między UE a państwem trzecim lub organizacją międzynarodową.

6. Umowy o bezpieczeństwie informacji przewidują techniczne uzgodnienia wykonawcze, dokonywane przez Biuro ds. Bezpieczeństwa SGR, dyrekcję ds. bezpieczeństwa Komisji Europejskiej oraz właściwe władze bezpieczeństwa danego państwa trzeciego lub danej organizacji międzynarodowej. Takie uzgodnienia wykonawcze uwzględniają stopień ochrony przewidziany w przepisach, strukturach i procedurach bezpieczeństwa istniejących w odnośnym państwie trzecim lub odnośnej organizacji międzynarodowej. Uzgodnienia te zatwierdzane są przez Komitet ds. Bezpieczeństwa.

7. Nie wymienia się żadnych informacji niejawnych UE drogą elektroniczną, o ile nie zostało to wyraźnie przewidziane w umowie o bezpieczeństwie informacji lub technicznych uzgodnieniach wykonawczych.

8. Umowy o bezpieczeństwie informacji przewidują, że przed wymianą informacji niejawnych na mocy umowy Biuro ds. Bezpieczeństwa SGR oraz dyrekcja ds. bezpieczeństwa Komisji Europejskiej zgodnie stwierdzają, że strona otrzymująca jest w stanie w satysfakcjonujący sposób chronić i zabezpieczać informacje jej dostarczone.

9. Gdy Rada zawiera umowę o bezpieczeństwie informacji, dla każdej ze stron umowy zostaje wyznaczona kancelaria tajna, do której – jako głównego punktu – będą wpływać i z której będą przekazywane informacje niejawne.

10. Aby ocenić skuteczność przepisów, struktur i procedur bezpieczeństwa w odnośnym państwie trzecim lub organizacji międzynarodowej, Biuro ds. Bezpieczeństwa SGR wraz z dyrekcją ds. bezpieczeństwa w Komisji Europejskiej oraz w porozumieniu z tym państwem trzecim lub organizacją międzynarodową przeprowadza wizyty oceniające. Wizyty takie przeprowadzane są zgodnie z odnośnymi przepisami załącznika IV i obejmują ocenę:

(a) ram prawnych mających zastosowanie do ochrony informacji niejawnych;

(b) wszelkich cech charakterystycznych polityki bezpieczeństwa oraz sposobu, w jaki zorganizowana jest polityka bezpieczeństwa w państwie trzecim lub organizacji międzynarodowej, co może mieć wpływ na to, jaki najwyższą klauzulę mogą mieć wymieniane informacje niejawne;

(c) rzeczywiście stosowanych środków i procedur bezpieczeństwa; oraz

(d) procedur poświadczania bezpieczeństwa osobowego dotyczących klauzuli informacji niejawnych UE, które mają być udostępniane.

11. Zespół przeprowadzający wizytę oceniającą w imieniu UE ocenia, czy obowiązujące w danym państwie trzecim lub organizacji międzynarodowej przepisy i procedury dotyczące bezpieczeństwa są odpowiednie do ochrony informacji niejawnych UE o określonej klauzuli.

12. Wnioski z takich wizyt przedstawiane są w sprawozdaniu, na którego podstawie Komitet ds. Bezpieczeństwa określa najwyższą klauzulę informacji niejawnych UE, które mogą być wymieniane z daną stroną trzecią w postaci papierowej, a w odpowiednich przypadkach elektronicznej, a także wszelkie szczególne warunki wymiany informacji z tą stroną.

13. Należy dołożyć wszelkich starań, by przeprowadzić pełną kontrolę bezpieczeństwa w danym państwie trzecim lub danej organizacji międzynarodowej, zanim Komitet ds. Bezpieczeństwa zatwierdzi uzgodnienia wykonawcze, aby określić charakter i skuteczność funkcjonującego tam systemu bezpieczeństwa. Jeśli jednak nie jest to możliwe, Komitet ds. Bezpieczeństwa otrzymuje od Biura ds. Bezpieczeństwa SGR możliwie najpełniejsze sprawozdanie, sporządzone w oparciu o posiadane przez to biuro informacje, w którym komitet informowany jest o mających zastosowanie przepisach dotyczących bezpieczeństwa oraz o sposobie organizacji kwestii bezpieczeństwa w danym państwie trzecim lub danej organizacji międzynarodowej.

14. Komitet ds. Bezpieczeństwa może zdecydować, że w oczekiwaniu na analizę wyników wizyty oceniającej nie można udostępnić żadnych informacji niejawnych UE lub można udostępnić te informacje tylko do określonego poziomu klauzuli; komitet może też przedstawić inne konkretne warunki dotyczące udostępniania informacji niejawnych UE danemu państwu trzeciemu lub danej organizacji międzynarodowej. Biuro ds. Bezpieczeństwa SGR powiadamia o tym dane państwo trzecie lub daną organizację międzynarodową.

15. Biuro ds. Bezpieczeństwa SGR, działając w porozumieniu z danym państwem trzecim lub daną organizacją międzynarodową, w regularnych odstępach czasu przeprowadza następne wizyty oceniające, aby sprawdzić, czy istniejące uzgodnienia nadal odpowiadają ustalonym minimalnym normom.

16. Po wejściu w życie umowy o bezpieczeństwie informacji i rozpoczęciu wymiany informacji niejawnych z danym państwem trzecim lub daną organizacją międzynarodową Komitet ds. Bezpieczeństwa może zdecydować o zmianie najwyższej klauzuli informacji niejawnych UE, które mogą być wymieniane w postaci papierowej lub elektronicznej, w szczególności w wyniku jednej z kolejnych wizyt oceniających.

IV. POROZUMIENIA ADMINISTRACYJNE

17. Jeżeli istnieje długoterminowa potrzeba wymiany z państwem trzecim lub organizacją międzynarodową informacji niejawnych o klauzuli z reguły nie wyższej niż RESTREINT UE i jeżeli Komitet ds. Bezpieczeństwa ustalił, że dana strona nie dysponuje wystarczająco rozwiniętym systemem bezpieczeństwa, tak aby było możliwe zawarcie umowy o bezpieczeństwie informacji, SG/WP może, z zastrzeżeniem zatwierdzenia przez Radę, zawrzeć porozumienie administracyjne z odnośnymi organami danego państwa trzeciego lub organizacji międzynarodowej.

18. Jeżeli z pilnych przyczyn operacyjnych należy szybko utworzyć ramy wymiany informacji niejawnych, Rada może wyjątkowo zdecydować o zawarciu porozumienia administracyjnego dotyczącego wymiany informacji o wyższej klauzuli.

19. Porozumienia administracyjne z reguły mają postać wymiany listów.

20. Przed faktycznym udostępnieniem informacji niejawnych UE danemu państwu trzeciemu lub danej organizacji międzynarodowej przeprowadzana jest wizyta oceniająca, o której mowa w pkt 10, a sprawozdanie przekazywane jest Komitetowi ds. Bezpieczeństwa, który ocenia je jako zadowalające. Jeżeli jednak istnieją wyjątkowe powody do pilnej wymiany informacji niejawnych UE, na które to powody zwraca się uwagę Rady, informacje niejawne UE mogą być udostępniane, pod warunkiem że dołoży się wszelkich starań, aby przeprowadzić taką kontrolę jak najszybciej.

21. Nie wymienia się żadnych informacji niejawnych UE drogą elektroniczną, o ile nie zostało to wyraźnie przewidziane w porozumieniu administracyjnym.

V. WYMIANA INFORMACJI NIEJAWNYCH W KONTEKŚCIE OPERACJI EPBiO

22. Umowy ramowe w sprawie udziału regulują uczestnictwo państw trzecich lub organizacji międzynarodowych w operacjach EPBiO. Umowy takie zawierają przepisy o udostępnianiu informacji niejawnych UE wytwarzanych do celów operacji EPBiO uczestniczącym w nich państwom trzecim lub organizacjom międzynarodowym. Najwyższy poziom klauzuli informacji niejawnych UE, które mogą być wymieniane, określany jest we wspólnym działaniu ustanawiającym każdą z operacji EPBiO.

23. Umowy *ad hoc* w sprawie udziału zawierane do celów konkretnej operacji EPBiO zawierają przepisy o udostępnianiu informacji niejawnych UE wytwarzanych do celów tej operacji uczestniczącemu w niej państwu trzeciemu lub organizacji międzynarodowej. Najwyższy poziom klauzuli informacji niejawnych UE, które mogą być wymieniane, określany jest we wspólnym działaniu ustanawiającym daną operację EPBiO.

24. Porozumienia administracyjne *ad hoc* dotyczące uczestnictwa państwa trzeciego lub organizacji międzynarodowej w konkretnej operacji EPBiO mogą obejmować m.in. udostępnianie temu państwu trzeciemu lub tej organizacji międzynarodowej informacji niejawnych UE wytworzonych do celów tej operacji. Porozumienia administracyjne *ad hoc* tego rodzaju są zawierane zgodnie z procedurami określonymi w sekcji IV pkt 17 i 18 powyżej. Najwyższy poziom klauzuli informacji niejawnych UE, które mogą być wymieniane, określany jest we wspólnym działaniu ustanawiającym daną operację EPBiO.

25. Przed wdrożeniem przepisów w sprawie udostępniania informacji niejawnych UE na warunkach określonych w pkt 22, 23 i 24 nie są wymagane uzgodnienia wykonawcze ani wizyty oceniające.

26. Jeśli państwo przyjmujące, na którego terytorium prowadzona jest operacja EPBiO, nie zawarło umowy o bezpieczeństwie informacji ani porozumienia administracyjnego z UE w zakresie wymiany informacji niejawnych, w przypadku konkretnej i natychmiastowej potrzeby operacyjnej można zawrzeć porozumienie administracyjne *ad hoc*. Możliwość ta przewidziana jest we wspólnym działaniu ustanawiającym operację EPBiO. Informacje niejawne UE udostępnione w tych okolicznościach ograniczone są do informacji wytworzonych do celów operacji EPBiO i mają klauzulę nie wyższą niż RESTREINT UE. Na mocy takiego porozumienia administracyjnego *ad hoc* państwo przyjmujące podejmuje się ochrony informacji niejawnych UE zgodnie z minimalnymi normami, które nie mogą być mniej rygorystyczne niż normy określone w niniejszej decyzji.

27. Przepisy dotyczące informacji niejawnych, które mają być zawarte w umowach ramowych w sprawie udziału, umowach *ad hoc* w sprawie udziału i porozumieniach administracyjnych *ad hoc*, o których mowa w pkt 22–24, przewidują, że dane państwo trzecie lub organizacja międzynarodowa dopilnowuje, by jego / jej personel oddelegowany do jakiejkolwiek operacji chronił informacje niejawne UE zgodnie z zasadami bezpieczeństwa Rady i korzystając z dalszych wskazówek wydanych przez właściwe organy, w tym strukturę dowodzenia operacji.

28. Jeśli uczestniczące w operacji państwo trzecie lub organizacja międzynarodowa zawrze następnie z UE umowę o bezpieczeństwie informacji, zastępuje ona wszelkie umowy ramowe w sprawie udziału, umowy *ad hoc* w sprawie udziału i porozumienia administracyjne *ad hoc* odnośnie do wymiany informacji niejawnych UE i pracy z ich wykorzystaniem.

29. Nie zezwala się na wymianę z państwem trzecim lub organizacją międzynarodową informacji niejawnych UE drogą elektroniczną na mocy umowy ramowej w sprawie udziału, umowy *ad hoc* w sprawie udziału i porozumienia administracyjnego *ad hoc*, o ile nie jest to wyraźnie przewidziane w tej umowie lub w tym porozumieniu.

30. Informacje niejawne UE wytworzone do celów operacji EPBiO mogą być udostępnianie pracownikom oddelegowanym do tej operacji przez państwa trzecie lub organizacje międzynarodowe. Upoważniając taki personel do dostępu do informacji niejawnych UE w obiektach lub w ramach CIS operacji EPBiO, należy odpowiednio zadbać o złagodzenie ryzyka utraty lub narażenia na szwank bezpieczeństwa informacji oraz zastosować służące temu środki (np. podział na jednostki, rejestracja udostępnianych informacji niejawnych UE).

VI. WYJĄTKOWE UDOSTĘPNIANIE *AD HOC* INFORMACJI NIEJAWNYCH UE

31. Jeśli nie ustanowiono ram zgodnie z powyższymi sekcjami III–V, a Rada lub jeden z jej organów przygotowawczych stwierdza, że istnieje wyjątkowa potrzeba udostępnienia informacji niejawnych UE państwu trzeciemu lub organizacji międzynarodowej, SGR:

(a) w miarę możliwości uzyskuje od władz bezpieczeństwa odnośnego państwa trzeciego lub odnośnej organizacji międzynarodowej potwierdzenie, że ich przepisy, struktury i procedury bezpieczeństwa gwarantują ochronę udostępnionych informacji niejawnych UE zgodnie z normami nie mniej rygorystycznymi niż normy określone w niniejszej decyzji;

(b) zwraca się do Komitetu ds. Bezpieczeństwa, by na podstawie dostępnych informacji wydał zalecenie dotyczące zaufania, jakie można pokładać w przepisach, strukturach i procedurach bezpieczeństwa w państwie trzecim lub organizacji międzynarodowej, którym mają zostać udostępnione informacje niejawne UE.

32. Jeśli Komitet ds. Bezpieczeństwa wyda zalecenie, by udostępnić informacje niejawne UE, sprawa zostaje przekazana COREPER-owi, który podejmuje decyzję o udostępnieniu tych informacji.

33. Jeśli Komitet ds. Bezpieczeństwa wyda zalecenie, by nie udostępniać informacji niejawnych UE:

(a) w sprawach odnoszących się do WPZiB/EPBiO Komitet Polityczny i Bezpieczeństwa omawia tę kwestię i formułuje zalecenie dotyczące decyzji COREPER-u;

(b) we wszystkich innych sprawach COREPER omawia tę kwestię i podejmuje decyzję.

34. We właściwych przypadkach i po uzyskaniu wcześniej pisemnej zgody wytwórcy informacji COREPER może postanowić o udostępnieniu informacji niejawnych wyłącznie częściowo lub wyłącznie pod warunkiem uprzedniego obniżenia lub zniesienia klauzuli tajności lub też pod warunkiem, że informacje, które mają zostać udostępnione, przygotowane zostaną bez odniesienia do źródła lub pierwotnej klauzuli tajności UE.

35. W następstwie decyzji o udostępnieniu informacji niejawnych UE, SGR przekazuje dany dokument, który jest opatrzony oznaczeniem dotyczącym możliwości jego udostępnienia, wskazującym państwo trzecie lub organizację międzynarodową, którym zostaje udostępniony. Przed faktycznym udostępnieniem lub w momencie udostępniania rzeczona strona trzecia na piśmie zobowiązuje się do ochrony informacji niejawnych UE, które otrzymuje, zgodnie z podstawowymi zasadami i minimalnymi normami przedstawionymi w niniejszej decyzji.

VII. UPOWAŻNIENIE DO UDOSTĘPNIANIA INFORMACJI NIEJAWNYCH UE PAŃSTWOM TRZECIM LUB ORGANIZACJOM MIĘDZYNARODOWYM

36. Jeżeli istnieją ramy wymiany informacji niejawnych z państwem trzecim lub organizacją międzynarodową zgodnie z pkt 2, Rada podejmuje decyzję upoważniającą SG/WP do udostępniania informacji niejawnych UE temu państwu trzeciemu lub organizacji międzynarodowej, z zachowaniem zasady uzyskania zgody wytwórcy.

37. Jeżeli istnieją ramy wymiany informacji niejawnych z państwem trzecim lub organizacją międzynarodową zgodnie z pkt 3, SG/WP upoważniony jest do udostępniania informacji niejawnych UE zgodnie ze wspólnym działaniem ustanawiającym daną operację EPBiO oraz z zachowaniem zasady uzyskania zgody wytwórcy.

38. SG/WP może przenieść takie upoważnienie na urzędników wysokiego szczebla w SGR lub inne osoby, których jest zwierzchnikiem.

DODATKI

DODATEK A

Definicje

DODATEK B

Odpowiedniki klauzul tajności

DODATEK C

Wykaz krajowych władz bezpieczeństwa (NSA)

DODATEK D

Wykaz skrótów

DEFINICJE

Do celów niniejszej decyzji zastosowanie mają następujące definicje:

„Akredytacja” oznacza formalny proces prowadzący do stwierdzenia przez organ ds. akredytacji bezpieczeństwa (SAA), że określony system jest zatwierdzony do celów działania na zdefiniowanym poziomie klauzuli tajności, w konkretnym trybie bezpieczeństwa w swoim środowisku operacyjnym oraz na poziomie ryzyka możliwym do zaakceptowania, przy założeniu, że wdrożony został zatwierdzony zestaw zabezpieczeń technicznych, fizycznych, organizacyjnych i proceduralnych;

„Strefa administracyjna” – zob. załącznik II pkt 12;

„Zasoby” oznaczają wszystkie elementy, które mają wartość dla danej organizacji, prowadzenia przez nią działań i ich ciągłości, w tym zasoby informacyjne, które wspierają misję organizacji;

„Naruszenie bezpieczeństwa” – zob. art. 13 ust. 1;

„Etapy istnienia CIS” oznaczają cały okres istnienia CIS, który obejmuje powstanie pomysłu, opracowanie koncepcji, zaplanowanie, analizę wymogów, zaprojektowanie, utworzenie, testowanie, wdrożenie, działanie, konserwację i wycofanie z działania;

„Umowa niejawna” oznacza umowę zawieraną przez SGR z wykonawcą na dostawę towarów, wykonanie robót lub świadczenie usług, co wymaga dostępu do informacji niejawnych UE lub wytwarzania takich informacji bądź wiąże się z dostępem do nich lub ich wytwarzaniem;

„Niejawna umowa o podwykonawstwo” oznacza umowę zawieraną przez wykonawcę SGR z innym wykonawcą (tj. podwykonawcą) na dostawę towarów, wykonanie robót lub świadczenie usług, co wymaga dostępu do informacji niejawnych UE lub wytwarzania takich informacji bądź wiąże się z dostępem do nich lub ich wytwarzaniem;

„System łączności i informacji” („CIS”) – zob. art. 9 ust. 2;

„Narażenie na szwank bezpieczeństwa” – zob. art. 13 ust. 2;

„Wykonawca” oznacza osobę fizyczną lub prawną posiadającą zdolność prawną do zawierania umów;

„Kryptogram” oznacza wynik szyfrowania informacji niejawnych UE przy pomocy zatwierdzonego produktu kryptograficznego;

„Materiał kryptograficzny” oznacza algorytmy kryptograficzne, sprzęt i oprogramowanie kryptograficzne, a także produkty zawierające szczegóły stosowania i związaną z nim dokumentację oraz klucze do symetrycznych lub asymetrycznych mechanizmów kryptograficznych;

„Specjalny bezpieczny tryb działania” oznacza tryb działania, w którym WSZYSTKIE osoby posiadające dostęp do systemu są sprawdzane do celów dostępu do informacji o najwyższej klauzuli tajności, jaki mają informacje wykorzystywane do pracy w ramach systemu, oraz podlegają wspólnej zasadzie ograniczonego dostępu w odniesieniu do WSZYSTKICH informacji wykorzystywanych do pracy w ramach tego systemu.

„Głęboka ochrona” oznacza stosowanie pakietu środków bezpieczeństwa o różnych poziomach obrony;

„Wyznaczona władza bezpieczeństwa” („DSA”) oznacza organ podporządkowany krajowym władzom bezpieczeństwa państwa członkowskiego, odpowiedzialny za informowanie podmiotów prowadzących działalność przemysłową lub inną o krajowej polityce w zakresie wszelkich kwestii związanych z bezpieczeństwem przemysłowym oraz za udzielanie wskazówek i pomocy w ich wdrażaniu. Zadania wyznaczonej władzy bezpieczeństwa mogą wykonywać krajowe władze bezpieczeństwa lub jakiekolwiek inne właściwe organy;

„Dokument” oznacza każdą utrwaloną informację, bez względu na jej formę fizyczną i cechy charakterystyczne;

„Obniżenie klauzuli tajności” oznacza obniżenie poziomu klauzuli tajności;

„Operacja EPBiO” oznacza wojskową lub cywilną operację zarządzania kryzysowego realizowaną na mocy tytułu V Traktatu o Unii Europejskiej;

„Informacje niejawne UE” – zob. art. 2 ust. 1;

„Świadectwo bezpieczeństwa przemysłowego” („FSC”) oznacza stwierdzenie przez NSA lub DSA w wyniku procedur administracyjnych, że z punktu widzenia bezpieczeństwa dany obiekt jest w stanie zapewnić właściwą ochronę informacji niejawnych UE do określonego poziomu klauzuli oraz że jego pracownicy, którzy potrzebują dostępu do informacji niejawnych UE, zostali właściwie sprawdzeni pod względem bezpieczeństwa oraz poinformowani o odpowiednich wymogach bezpieczeństwa niezbędnych do uzyskania dostępu do informacji niejawnych UE i do ich ochrony;

„Praca z wykorzystaniem” informacji niejawnych UE oznacza wszelkie możliwe działania, którym mogą podlegać informacje niejawne UE na wszystkich etapach istnienia. Pojęcie to obejmuje wytwarzanie tych informacji, ich przetwarzanie, przewożenie, obniżanie klauzul, znoszenie klauzul oraz niszczenie. W przypadku CIS, obejmuje ono także gromadzenie informacji, ich przedstawianie, przekazywanie i przechowywanie;

„Posiadacz” oznacza osobę posiadającą odpowiednie uprawnienia i podlegającą zasadzie ograniczonego dostępu, znajdującą się w posiadaniu informacji niejawnych UE i w związku z tym odpowiedzialną za ich ochronę;

„Podmiot prowadzący działalność przemysłową lub inną” oznacza podmiot zajmujący się dostawą towarów, wykonywaniem robót lub świadczeniem usług; może to być podmiot prowadzący działalność przemysłową, handlową, usługową, naukową, badawczą, edukacyjną lub rozwojową lub osoba prowadząca własną działalność;

„Bezpieczeństwo przemysłowe” – zob. art. 11 ust. 1;

„Informacje” oznaczają wiedzę, którą można przekazać w dowolnej postaci;

„Zabezpieczanie informacji” – zob. art. 9 ust. 1;

„Połączenie międzysystemowe” – zob. załącznik III pkt 31;

„Zarządzanie informacjami niejawnymi” – zob. art. 10 ust. 1;

„Materiały” oznaczają jakikolwiek dokument lub dowolny mechanizm lub sprzęt, już wytworzone lub będące w trakcie wytwarzania;

„Wielopoziomowy bezpieczny tryb działania” oznacza tryb działania, w którym NIE WSZYSTKIE osoby posiadające dostęp do CIS są sprawdzane do celów dostępu do informacji o najwyższym poziomie klauzuli tajności, jaki mają informacje wykorzystywane do pracy w ramach tego systemu, oraz NIE WSZYSTKIE osoby posiadające dostęp do systemu podlegają wspólnej zasadzie ograniczonego dostępu w odniesieniu do informacji wykorzystywanych do pracy w ramach tego CIS.

„Wytwórca” oznacza instytucję, agencję lub organ UE, państwo członkowskie, państwo trzecie lub organizację międzynarodową, pod nadzorem której wytworzono informacje niejawne lub wprowadzono je do struktur UE;

„Bezpieczeństwo osobowe” – zob. art. 7 ust. 1;

„Poświadczenie bezpieczeństwa osobowego” („PBO”) oznacza jedno lub oba z poniższych:

- „poświadczenie bezpieczeństwa osobowego UE” („PBO UE”) do celów dostępu do informacji niejawnych UE oznacza decyzję administracyjną organu powołującego SGR podjętą zgodnie z niniejszą decyzją po przeprowadzeniu przez właściwe organy państwa członkowskiego postępowania sprawdzającego, w której to decyzji poświadcza się, że danej osobie można do określonej daty udzielać dostępu do informacji niejawnych UE do określonego poziomu klauzuli (CONFIDENTIEL UE lub wyższej), pod warunkiem że stwierdzono, iż osoba ta podlega zasadzie ograniczonego dostępu; o takiej osobie mówi się, że została „sprawdzona pod względem bezpieczeństwa”;

- „krajowe poświadczenie bezpieczeństwa osobowego” („krajowe PBO”) do celów dostępu do informacji niejawnych UE oznacza decyzję administracyjną właściwego organu państwa członkowskiego podejmowaną po przeprowadzeniu przez właściwe organy państwa członkowskiego postępowania sprawdzającego, w której to decyzji zaświadcza się, że danej osobie można do określonej daty udzielać dostępu do informacji niejawnych UE do określonego poziomu klauzuli (CONFIDENTIEL UE lub wyższej), pod warunkiem że stwierdzono, iż osoba ta podlega zasadzie ograniczonego dostępu; o takiej osobie mówi się, że została „sprawdzona pod względem bezpieczeństwa”;

„Certyfikat potwierdzający posiadanie poświadczenia bezpieczeństwa osobowego” („CPBO”) oznacza wydany przez właściwy organ certyfikat potwierdzający, że dana osoba została sprawdzona pod względem bezpieczeństwa i posiada ważne krajowe PBO lub PBO UE, oraz określający poziom klauzuli tajności informacji niejawnych UE, do jakich osoba ta może mieć dostęp (CONFIDENTIEL UE lub wyższy), okres ważności odnośnego PBO oraz okres ważności samego certyfikatu.

„Bezpieczeństwo fizyczne” – zob. art. 8 ust. 1;

„Instrukcje bezpieczeństwa programu/projektu” („PSI”) oznaczają wykaz procedur bezpieczeństwa stosowanych do określonego programu/projektu w celu ujednolicenia procedur bezpieczeństwa. Instrukcje mogą być zmieniane podczas trwania programu/projektu;

„Rejestracja” – zob. załącznik IV pkt 17;

„Ryzyko szczątkowe” oznacza ryzyko, które pozostaje po wdrożeniu środków bezpieczeństwa w CIS, przy założeniu, że nie przeciwdziała się wszystkim zagrożeniom i że nie wszystkie słabe punkty można wyeliminować;

„Ryzyko” oznacza prawdopodobieństwo, że dane zagrożenie wykorzysta wewnętrzne i zewnętrzne narażenia danej organizacji lub jakiegokolwiek systemu, z którego korzysta, i tym samym spowoduje szkody dla tej organizacji i jej materialnych lub niematerialnych zasobów. Ryzyko mierzone jest jako połączenie prawdopodobieństwa wystąpienia zagrożeń oraz ich skutków.

- „Akceptacja ryzyka” jest decyzją o zaakceptowaniu dalszego występowania określonego ryzyka szczątkowego po zmniejszeniu ryzyka;

- „Ocena ryzyka” polega na określaniu zagrożeń i narażeń oraz przeprowadzeniu odnośnej analizy ryzyka, tj. analizy prawdopodobieństwa i skutków;

- „Powiadamianie o ryzyku” polega na upowszechnianiu wiedzy o ryzyku wśród społeczności korzystających z CIS, na informowaniu o takim ryzyku organów zatwierdzających i na składaniu sprawozdań z nich organom operacyjnym;

- „Zmniejszanie ryzyka” polega na łagodzeniu, usuwaniu lub redukowaniu ryzyka (przy pomocy odpowiedniego połączenia środków technicznych, fizycznych, organizacyjnych lub proceduralnych), przenoszeniu lub monitorowaniu ryzyka;

„Strefa zabezpieczona” – zob. załącznik II pkt 12;

„Dokument określający aspekty bezpieczeństwa” („SAL”) oznacza zbiór specjalnych warunków umownych, wydany przez instytucję zamawiającą, stanowiący integralną część jakiejkolwiek umowy niejawnej obejmującej dostęp do informacji niejawnych UE lub ich wytwarzanie, określający wymogi bezpieczeństwa lub wskazujący te elementy umowy, których bezpieczeństwo wymaga ochrony;

„Przewodnik nadawania klauzul” („SCG”) oznacza dokument opisujący niejawne elementy programu lub umowy i określający mające zastosowanie poziomy klauzul. SCG może być rozszerzany podczas trwania programu lub umowy, a klauzule tajności dla części informacji mogą zostać zmienione lub obniżone; jeżeli SCG jest opracowany, to powinien być częścią dokumentu określającego aspekty bezpieczeństwa;

„Postępowanie sprawdzające w zakresie bezpieczeństwa” oznacza procedury dochodzeniowe przeprowadzane przez właściwy organ danego państwa członkowskiego zgodnie z jego przepisami ustawowymi i wykonawczymi w celu uzyskania pewności, że nie istnieją żadne niekorzystne okoliczności, które mogłyby stanowić przeszkodę do udzielenia danej osobie krajowego PBO lub PBO UE do celów dostępu do informacji niejawnych UE do określonego poziomu klauzuli (CONFIDENTIEL UE lub wyższej);

„Bezpieczny tryb działania” oznacza określenie warunków działania CIS na podstawie klauzul informacji wykorzystywanych do pracy oraz poziomów poświadczeń jego użytkowników, ich formalnych zatwierdzeń dostępu oraz podlegania zasadzie ograniczonego dostępu. Istnieją trzy tryby działania, jeżeli chodzi o pracę z wykorzystaniem informacji niejawnych lub przekazywanie ich: tryb specjalny, tryb wzmożony i tryb wielopoziomowy;

„Proces kontroli ryzyka dla bezpieczeństwa” oznacza cały proces określania, kontrolowania i minimalizacji występowania związanych z ryzykiem wydarzeń, które mogą wpłynąć na daną organizację lub jakikolwiek system przez nią używany. Obejmuje on wszystkie działania związane z ryzykiem, w tym ocenę, zmniejszanie, akceptację i powiadamianie;

„Wzmożony bezpieczny tryb działania” oznacza tryb działania, w którym WSZYSTKIE osoby posiadające dostęp do systemu są sprawdzane do celów dostępu do informacji o najwyższym poziomie klauzuli tajności, jaki mają informacje wykorzystywane do pracy w ramach systemu, lecz NIE WSZYSTKIE osoby posiadające dostęp do systemu podlegają wspólnej zasadzie ograniczonego dostępu w odniesieniu do informacji wykorzystywanych do pracy w ramach tego systemu;

„Zagrożenie” oznacza potencjalną przyczynę niepożądanego incydentu, który może skutkować szkodą dla organizacji lub jakiegokolwiek systemu przez nią używanego; zagrożenia takie mogą być przypadkowe lub zamierzone (rozmyślne) i obejmują elementy zagrażające, potencjalne cele i metody ataku;

„Narażenie” oznacza każdego rodzaju słaby punkt, który może zostać wykorzystany przez jedno zagrożenie lub większą ich liczbę. Narażenie może być zaniechaniem lub może odnosić się do słabych punktów środków kontroli, jeśli chodzi o ich solidność, wszechstronność lub spójność; narażenie może mieć charakter techniczny, proceduralny, fizyczny, organizacyjny lub operacyjny.

DODATEK B

ODPOWIEDNIKI KLAUZUL TAJNOŚCI

UE	TRES SECRET UE	SECRET UE	CONFIDENTIEL UE	RESTREINT UE
Belgia	Très Secret (Loi 11.12.1998) Zeer Geheim (Wet 11.12.1998)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998)	*uwaga[1] poniżej*
Bułgaria	Строго секретно	Секретно	Поверително	За служебно ползване
Republika Czeska	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Dania	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Niemcy	Streng geheim	Geheim	VS[2]— Vertraulich	VS — Nur für den Dienstgebrauch
Estonia	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Grecja	Άκρως Απόρρητο Skrót: ΑΑΠ	Απόρρητο Skrót: (ΑΠ)	Εμπιστευτικό Skrót: (ΕΜ)	Περιορισμένης Χρήσης Skrót: (ΠΧ)
Hiszpania	Secreto	Reservado	Confidencial	Difusión Limitada
Francja	Très Secret Défense	Secret Défense	Confidentiel Défense	*uwaga[3] poniżej*
Irlandia	Top Secret	Secret	Confidential	Restricted
Włochy	Segretissimo	Segreto	Riservatissimo	Riservato
Cypr	Άκρως Απόρρητο Skrót: (ΑΑΠ)	Απόρρητο Skrót: (ΑΠ)	Εμπιστευτικό Skrót: (ΕΜ)	Περιορισμένης Χρήσης Skrót: (ΠΧ)
Łotwa	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Litwa	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luksemburg	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Węgry	Szigorúan titkos!	Titkos!	Bizalmas!	Korlátozott terjesztésű!
Malta	L-Oghla Segretezza	Sigriet	Kunfidenzjali	Ristrett
Niderlandy	Stg ZEER GEHEIM	Stg GEHEIM	Stg CONFIDENTIEEL	Dep VERTROUWELIJK
Austria	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Polska	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugalia	Muito Secreto	Secreto	Confidencial	Reservado
Rumunia	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu
Słowenia	Strogo tajno	Tajno	Zaupno	Interno
Słowacja	| Prísne tajné	Tajné	Dôverné	Vyhradené
Finlandia	ERITTÄIN SALAINEN	SALAINEN	LUOTTAMUKSELLINEN	KÄYTTÖ RAJOITETTU
Szwecja[4]	Hemlig/Top secret Hemlig av synnerlig betydelse för rikets säkerhet	Hemlig/Secret Hemlig	Hemlig/Confidential Hemlig	Hemlig/Restricted Hemlig
Zjednoczone Królestwo	Top Secret	Secret	Confidential	Restricted

[1] Oznaczenie Restreinte / Beperkte Verspreiding nie jest w Belgii uznawane za klauzulę tajności. W Belgii pracuje się z wykorzystaniem informacji oznaczonych „RESTREINT UE" i chroni je w sposób nie mniej rygorystyczny, niż przewidują to normy i procedury opisane w zasadach bezpieczeństwa Rady Unii Europejskiej.

[2] Niemcy: VS = Verschlusssache.

[3] Francja nie stosuje klauzuli „RESTREINT" w swoim systemie krajowym. We Francji pracuje się z wykorzystaniem informacji oznaczonych „RESTREINT UE" i chroni je w sposób nie mniej rygorystyczny, niż przewidują to standardy i procedury opisane w zasadach bezpieczeństwa Rady Unii Europejskiej.

[4] Szwecja: oznaczenia towarzyszące klauzulom tajności w górnym rzędzie są używane przez organy obrony, zaś oznaczenia w dolnym rzędzie – przez inne organy.

WYKAZ KRAJOWYCH WŁADZ BEZPIECZEŃSTWA (NSA)

BELGIA

Autorité nationale de Sécurité
SPF Affaires étrangères, Commerce extérieur
et Coopération au Développement
15, rue des Petits Carmes
B-1000 Bruxelles
Telefon sekretariatu: + 32/2/501 45 42
Faks: + 32/2/501 45 96

BUŁGARIA

State Commission on Information Security
1A Angel Kanchev Str.
BG-1000 Sofia
Telefon: + 359/2/921 5911
Faks: + 359/2/987 3750
E-mail: dksi@government.bg
Strona internetowa: www.dksi.bg

REPUBLIKA CZESKA

Národní bezpečnostní úřad
(krajowe władze bezpieczeństwa)
Na Popelce 2/16
CZ-150 06 Praha 56
Telefon: + 420/257 28 33 35
Faks: + 420/257 28 31 10
E-mail: czech.nsa@nbu.cz
Strona internetowa: www.nbu.cz

DANIA

Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
DK-2860 Søborg
Telefon: + 45/33/14 88 88
Faks: + 45/33/43 01 90

Forsvarets Efterretningstjeneste
(Danish Defence Intelligence Service)
Kastellet 30
DK-2100 Copenhagen Ø
Telefon: + 45/33/32 55 66
Faks: + 45/33/93 13 20

NIEMCY

Bundesministerium des Innern
Referat ÖS III 3
Alt-Moabit 101 D
D-11014 Berlin
Telefon: + 49/30/18 681 1522
Faks: + 49/30/18 681 1441

ESTONIA

National Security Authority Department
Estonian Ministry of Defence
Sakala 1
15094 Tallinn, Estonia
Telefon: +372/7170 113, +372/7170 117
Faks: +372/7170 213
E-mail: nsa@kmin.ee

GRECJA

Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Διακλαδική Διεύθυνση Στρατιωτικών
Πληροφοριών (ΔΔΣΠ)
Διεύθυνση Ασφαλείας και Αντιπληροφοριών
ΣΤΓ 1020 -Χολαργός (Αθήνα)
Ελλάδα
Τηλέφωνα: + 30/210/657 20 45 (ώρες
γραφείου)
+ 30/210/657 20 09 (ώρες γραφείου)
Φαξ: + 30/210/653 62 79
+ 30/210/657 76 12

Hellenic National Defence General Staff
(HNDGS)
Military Intelligence Sectoral Directorate
Security Counterintelligence Directorate
GR-STG 1020 Holargos – Athens
Telefon: + 30/210/657 20 45
+ 30/210/657 20 09
Faks: + 30/210/653 62 79
+ 30/210/657 76 12

HISZPANIA

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
E-28023 Madrid
Telefon: + 34/91/372 50 00
Faks: + 34/91/372 58 08
E-mail: nsa-sp@areatec.com

FRANCJA

Secrétariat général de la Défense Nationale
Service de Sécurité de Défense (SGDN/SSD)
51 Boulevard de la Tour-Maubourg
F-75700 Paris 07 SP
Telefon: + 33/1/71 75 81 77
Faks: + 33/1/71 75 82 00

IRLANDIA

National Security Authority
Department of Foreign Affairs
76 - 78 Harcourt Street
Dublin 2
Irlandia
Telefon: + 353/1/ 478 08 22
Faks: + 353/1/ 408 29 59

WŁOCHY

Presidenza del Consiglio dei Ministri
Autorità Nazionale per la Sicurezza
D.I.S. - U.C.Se.
Via di Santa Susanna, 15
I-1187 Roma
Telefon: + 39/06/611 742 66
Faks: + 39/06/488 52 73

CYPR

ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Υπουργείο Άμυνας
Λεωφόρος Εμμανουήλ Ροΐδη 41432
Λευκωσία, Κύπρος
Τηλέφωνα: + 357/22/80 75 69, + 357/22/80 76 43, + 357/22/80 77 64, + 357/99 35 80 00
Τηλεομοιότυπο: + 357/22/30 23 51

Ministry of Defence
Minister's Military Staff
National Security Authority (NSA)
4 Emanuel Roidi street
CY-1432 Nicosia
Telefon: + 357/22/80 75 69, + 357/22/80 76 43, +357 /22/80 77 64, + 357/99 35 80 00
Faks: + 357/22/30 23 51

ŁOTWA

National Security Authority
Constitution Protection Bureau of the Republic of Latvia
P.O.Box 286
LV 1001, Riga
Telefon: +371/6702 54 18
Faks: +371/6702 54 54
E-mail: ndi@sab.gov.lv

LITWA

National Security Authority of the Republic of Lithuania
Gedimino 40/1
LT-2600 Vilnius
Telefon: + 370/5/266 32 05
Faks: + 370/5/266 32 00

LUKSEMBURG

Autorité nationale de Sécurité
Boîte postale 2379
L-1023 Luxembourg
Telefon: + 352/2478 22 10 central
+ 352/2478 22 53 direct
Faks: + 352/2478 22 43

WĘGRY

Nemzeti Biztonsági Felügyelet
P.O. Box 2
HU-1357 Budapest
Telefon: + 361/346 96 52
Faks: + 361/346 96 58
Strona internetowa: www.nbf.hu

MALTA

Ministry of Justice and Home Affairs
P.O. Box 146
MT-Valletta
Telefon: + 356/21 24 98 44
Faks: + 356/25 69 53 21

NIDERLANDY

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20010
NL-2500 EA Den Haag
Telefon: + 31/70/320 44 00
Faks: + 31/70/320 07 33

Ministerie van Defensie
Beveiligingsautoriteit
Postbus 20701
NL-2500 ES Den Haag
Telefon: + 31/70/318 70 60
Faks: + 31/70/318 75 22

AUSTRIA

Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
A-1014 Wien
Telefon: + 43/1/531 15 25 94
Faks: + 43/1/531 15 26 15

POLSKA

Internal Security Agency
(Agencja Bezpieczeństwa Wewnętrznego – ABW)
ul. Rakowiecka 2A
00-993 Warszawa
Telefon: + 48/22/585 73 60
Faks: + 48/22/585 85 09
E-mail: nsa@abw.gov.pl
Strona internetowa: www.abw.gov.pl

Military Counter-Intelligence Service
(Służba Kontrwywiadu Wojskowego)
Biuro Ochrony Informacji Niejawnych
Oczki 1
02-007 Warszawa
Telefon: + 48/22/684 12 47
Faks: + 48/22/684 10 76
E-mail: skw@skw.gov.pl

PORTUGALIA

Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Rua da Junqueira, 69
1300-342 Lisboa
Telefon: +351/ 213 031 710
Faks: +351/ 213 031 711

RUMUNIA

Romanian NSA - ORNISS
National Registry Office for Classified Information
Oficiul Registrului Național al Informațiilor Secrete de Stat
4 Mures Street
RO-012275 Bucharest
Telefon: 00 4 021 224 58 30
Faks: 00 4 021 224 07 14

SŁOWENIA

Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
SVN-1000 Ljubljana
Telefon: + 386/1/478 13 90
Faks: + 386/1/478 13 99

SŁOWACJA

Národný bezpečnostný úrad
(krajowe władze bezpieczeństwa)
Budatínska 30
P.O. Box 16
SVK-850 07 Bratislava
Telefon: + 421/2/68 69 23 14
Faks: + 421/2/63 82 40 05

FINLANDIA

National Security Authority
Ministry for Foreign Affairs
P.O. Box 453
FI-00023 Government
Telefon: + 358/9/160 56487
Faks: + 358/9/160 56494
E-mail: NSA@formin.fi

SZWECJA
Utrikesdepartementet
SSSB
S-103 39 Stockholm
Telefon: + 46/8/405 54 44
Faks: + 46/8/723 11 76

ZJEDNOCZONE KRÓLESTWO

UK National Security Authority
PO Box 60628
London SW1P 9HA
Telefon: + 44/(0)20 7233 8181
Faks: + 44/(0)20 7233 818

DODATEK D

LIST OF ABBREVIATIONS

Acronym	Meaning
AQUA	Appropriately Qualified Authority
BPS	Boundary Protection Services
CAA	Crypto Approval Authority
CCTV	Closed Circuit Television
CDA	Crypto Distribution Authority
CFSP	Common Foreign and Security Policy
CIS	Communication and Information Systems
DSA	Designated Security Authority
ESDP	European Security and Defence Policy
EUCI	EU Classified Information
EUSR	EU Special Representative
FSC	Facility Security Clearance
GSC	General Secretariat of the Council
IA	Information Assurance
IDS	Intrusion Detection System
IT	Information Technology
NSA	National Security Authority
PSCC	Personnel Security Clearance Certificate
PSI	Programme/Project Security Instructions
SAA	Security Accreditation Authority
SAB	Security Accreditation Board
SAL	Security Aspects Letter
SecOPs	Security Operating Procedures
SCG	Security Classification Guide
SG/HR	Secretary-General of the Council/High Representative for the CFSP
SSRS	System-Specific Security Requirement Statement