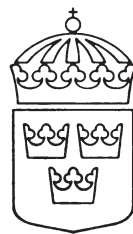


Sveriges internationella överenskommelser



ISSN 1102-3716

Utgiven av utrikesdepartementet

SÖ 2012:23

Nr 23

**Generellt säkerhetsskyddsavtal med Irland om
ömsesidigt skydd av säkerhetsskyddsklassificerade
försvarsrelaterade uppgifter
Stockholm och Dublin den 15 juni och den 16 juli
2012**

Regeringen beslutade den 20 oktober 2011 att underteckna avtalet. Avtalet trädde i kraft den 16 juli 2012.

**GENERELLT SÄKERHETSSKYDDSAVTAL MELLAN
KONUNGARIKET SVERIGES REGERING
OCH
IRLANDS REGERING
OM
ÖMSESIDIGT SKYDD
AV SÄKERHETSSKYDDSKLASSIFICERADE
FÖRSVARRELATERADE UPPGIFTER**

INLEDNING

Konungariket Sveriges regering och Irlands regering, nedan kallade *parterna*, har, med hänsyn till nationens säkerhet och i syfte att trygga skyddet av säkerhetsskyddsklassificerade försvarsrelaterade uppgifter som utbyts mellan dem, kommit överens om följande.

**ARTIKEL 1
DEFINITIONER**

I detta avtal gäller följande definitioner:

1. *säkerhetsskyddsklassificerad försvarsrelaterad uppgift*: försvarsrelaterad uppgift som enligt respektive parts lagstiftning oavsett form kräver skydd mot förlust, otillåtet röjande eller annan blottläggning och som har klassificerats som sådan.

2. *ursprungspart*: den part, inbegripet alla offentliga och privata aktörer inom dess jurisdiktion, som överför de säkerhetsskyddsklassificerade försvarsrelaterade uppgifterna till den andra parten.

3. *mottagande part*: den part, inbegripet alla offentliga och privata aktörer inom dess jurisdiktion, som tar emot de säkerhetsskyddsklassificerade försvarsrelaterade uppgifterna från den andra parten.

4. *tredje part*: en stat, inbegripet alla offentliga och privata aktörer inom dess jurisdiktion, eller en internationell organisation som inte är part i detta avtal.

5. *säkerhetsskyddsklassificerat kontrakt*: ett kontrakt som innehåller eller hänför sig till säkerhetsskyddsklassificerade försvarsrelaterade uppgifter.

6. *säkerhetsgodkännande*: ett positivt beslut efter registerkontroll som klarlägger att en fysisk eller juridisk person är lojal och i övrigt pålitlig från säkerhetssynpunkt i enlighet med nationella lagar och andra författningar.

7. *principen om behovsgrundad behörighet*: behovet av att få ta del av säkerhetsskyddsklassificerade försvarsrelaterade uppgifter för att kunna utföra sitt arbete.

**ARTIKEL 2
SÄKERHETSSKYDDSKLASSIFICERINGAR**

1. Säkerhetsskyddsklassificerade försvarsrelaterade uppgifter som lämnas ut i enlighet med detta avtal ska förses med lämplig säkerhetsskyddsmarkering enligt någon av parternas nationella lagar och andra författningar. Mottagna säkerhetsskyddsklassificerade försvarsrelaterade uppgifter ska skyddas

i enlighet med den nivå för säkerhetsskyddsklassificering som anges i punkt 2.

SÖ 2012:23

2. De nationella säkerhetsskyddsmarkeringarna motsvarar varandra enligt följande:

I Konungariket Sverige

I Irland

Försvarsmyndigheter	Andra myndigheter	Försvarsmyndigheter
HEMLIG/TOP SECRET	HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	TOP SECRET
HEMLIG/SECRET	HEMLIG	SECRET
HEMLIG/CONFIDENTIAL	–	CONFIDENTIAL
HEMLIG/RESTRICTED	–	RESTRICTED

3. Uppgifter från Konungariket Sverige som endast bär beteckningen "HEMLIG" ska i Irland behandlas som "SECRET" om inte ursprungsparten begär något annat.

4. Ursprungsparten ska utan dröjsmål meddela den mottagande parten om säkerhetsskyddsklassificeringen ändras för de utlämnade säkerhetsskyddsklassificerade försvarsrelaterade uppgifterna.

**ARTIKEL 3
BEHÖRIGA SÄKERHETSMYNDIGHETER**

1. Följande myndigheter är enligt detta avtal behöriga säkerhetsmyndigheter:

I Konungariket Sverige:

Försvarsmakten

Militära säkerhetstjänsten (nationell säkerhetsmyndighet för försvarsfrågor)

Försvarets materielverk (utsedd myndighet för industriella säkerhetsfrågor)

I Irland:

Försvarsdepartementet

2. Parterna ska förse varandra med nödvändiga kontaktuppgifter till sina respektive behöriga säkerhetsmyndigheter.

**ARTIKEL 4
RÖJANDE OCH ANVÄNDNING AV
SÄKERHETSSKYDDSKLASSIFICERADE
FÖRSVARRELATERADE UPPGIFTER**

1. Den mottagande parten ska vidta alla lagliga åtgärder för att förhindra att de utlämnade säkerhetsskyddsklassificerade försvarsrelaterade uppgifterna

röjs eller används för annat än för de syften och med de begränsningar som ursprungsparten har angett.

2. Den mottagande parten får i enlighet med sina nationella lagar endast lämna ut säkerhetsskyddsklassificerade försvarsrelaterade uppgifter på begäran av en tredje part efter att ursprungsparten uttryckligen skriftligen har medgett detta.

ARTIKEL 5

TILLGÅNG TILL SÄKERHETSSKYDDSKLASSIFICERADE FÖRSVARRELATERADE UPPGIFTER

1. Rätten att ta del av säkerhetsskyddsklassificerade försvarsrelaterade uppgifter ska i enlighet med principen om behovsgrundad behörighet och parternas respektive nationella standarder vara förbehållen personer

a) som har genomgått säkerhetsprövning och godkänts för lämplig klassificeringsnivå och

b) som har informerats om hur säkerhetsskyddsklassificerade försvarsrelaterade uppgifter skyddas.

2. Om formföreskrifterna i den nationella lagstiftningen är uppfyllda ska parterna erkänna varandras intyg om säkerhetsgodkännande.

ARTIKEL 6

SKYDD AV SÄKERHETSSKYDDSKLASSIFICERADE FÖRSVARRELATERADE UPPGIFTER

1. Ursprungsparten ska

a) se till att säkerhetsskyddsklassificerade försvarsrelaterade uppgifter som överlämnas förses med lämplig nationell säkerhetsskyddsmarkering i enlighet med artikel 2.2,

b) i förekommande fall informera den mottagande parten om eventuella villkor för utlämnandet eller begränsningar i användningen av de säkerhetsskyddsklassificerade försvarsrelaterade uppgifterna,

c) informera den mottagande parten om efterföljande ändringar av säkerhetsskyddsklassificeringen för de överförda säkerhetsskyddsklassificerade försvarsrelaterade uppgifterna.

2. Den mottagande parten ska

a) ge alla säkerhetsskyddsklassificerade försvarsrelaterade uppgifter det säkerhetsskydd som är likvärdigt med det skydd som ursprungsparten ger,

b) se till att säkerhetsskyddsklassificeringarna inte ändras utan skriftligt tillstånd från ursprungsparten.

ARTIKEL 7

ÖVERFÖRING AV SÄKERHETSSKYDDSKLASSIFICERADE FÖRSVARRELATERADE UPPGIFTER

1. Säkerhetsskyddsklassificerade försvarsrelaterade uppgifter ska överföras mellan parterna i enlighet med ursprungspartens nationella lagar och andra författningar på diplomatisk väg eller på annat sätt som de behöriga säkerhetsmyndigheterna kommer överens om.

2. Parterna kan ingå separata avtal om kommunikation/säkerhetsskydd för att fastställa en säker kommunikation sinsemellan.

ARTIKEL 8 BESÖK

1. Besök vid verksamhetsställen där säkerhetsskyddsklassificerade försvarsrelaterade uppgifter hanteras eller förvaras ska godkännas i förväg av värdpartens behöriga säkerhetsmyndigheter om inte något annat har överenskommit.

2. Framställningar om besök ska normalt lämnas till värdpartens behöriga säkerhetsmyndigheter minst en kalendermånad före besöket. De ska innehålla följande uppgifter:

a) Besökarens namn, födelsedatum och födelseort, medborgarskap, passnummer och en kopia av det intyg som visar att besökaren är säkerhetsgodkänd.

b) Närmare information om besökarens befattning.

d) Information om verksamhetsstället och/eller vilka personer som ska besökas.

e) Syftet med besöket.

g) Besökets/besökens tidpunkt och längd.

3. Säkerhetsskyddsklassificerade försvarsrelaterade uppgifter som röjs eller görs tillgängliga för besökare från en part ska behandlas som om de överförts till den parten och ska skyddas på vederbörligt sätt. Alla besökare ska uppfylla värdpartens säkerhetsskyddsföreskrifter.

ARTIKEL 9 SÄKERHETSSKYDDSKLASSIFICERADE KONTRAKT

1. Parterna ska erkänna varandras intyg om säkerhetsgodkännande av verksamhetsställe. De behöriga säkerhetsmyndigheterna får begära att det ska genomföras en säkerhetsskyddsinspektion på den andra partens verksamhetsställe för att försäkra sig om att säkerhetsskyddsnormerna fortsatt följer den partens nationella lagar och andra författningar.

2. Ett säkerhetsskyddsklassificerat kontrakt ska innehålla riktlinjer om säkerhetsskyddskraven och klassificeringen av varje aspekt av eller del i det säkerhetsskyddsklassificerade kontraktet.

ARTIKEL 10 SAMARBETE OM SÄKERHETSSKYDD för säkerhetsskyddsklassificerade försvarsrelaterade uppgifter

1. För att uppnå och bibehålla ett likvärdigt säkerhetsskydd får de behöriga säkerhetsmyndigheterna på begäran informera varandra om de nationella säkerhetsnormer, säkerhetsförfaranden och säkerhetsrutiner som tillämpas för att skydda säkerhetsskyddsklassificerade försvarsrelaterade uppgifter. De behöriga säkerhetsmyndigheterna får besöka varandra i detta syfte.

2. De behöriga säkerhetsmyndigheterna ska i förekommande fall informera varandra om aktuella säkerhetsrisker som kan äventyra de överförda säkerhetsskyddsklassificerade försvarsrelaterade uppgifterna.

3. De behöriga säkerhetsmyndigheterna får i enlighet med sina nationella lagar och andra författningar på begäran hjälpa varandra med att genomföra förfarandena för säkerhetsgodkännande.

4. Om någon av de behöriga säkerhetsmyndigheterna upphäver eller vidtar åtgärder för att upphäva den rätt att ta del av säkerhetsskyddsklassificerade försvarsrelaterade uppgifter som en medborgare i den andra parten har beviljats med stöd av ett säkerhetsgodkännande ska den andra parten underrättas och delges motiven för dessa åtgärder.

ARTIKEL 11

FÖRLUST, OBEHÖRIG ÅTKOMST TILL ELLER OTILLÅTET RÖJANDE AV SÄKERHETSSKYDDSKLASSIFICERADE FÖRSVARRELATERADE UPPGIFTER

1. I händelse av förlust, obehörig åtkomst till eller otillåtet röjande av säkerhetsskyddsklassificerade försvarsrelaterade uppgifter eller vid misstanke om detta ska den mottagande partens behöriga säkerhetsmyndighet omedelbart skriftligen informera ursprungspartens behöriga säkerhetsmyndighet.

2. Lämpliga myndigheter i den mottagande parten (vid behov biträdda av ursprungspartens behöriga myndigheter) ska omedelbart undersöka händelsen i enlighet med sina nationella lagar och andra författningar. Den mottagande parten ska utan dröjsmål informera ursprungsparten om omständigheterna kring händelsen, möjliga konsekvenser för säkerhetsskyddet, vilka åtgärder som har vidtagits för att begränsa förlusten eller skadan och resultatet av undersökningen.

ARTIKEL 12

TOLKNING OCH TVISTER

1. Detta avtal är avsett att följa parternas nationella lagar och internationell rätt. Om dessa är motstridiga ska tillämplig nationell lagstiftning gälla.

2. Tvister om tolkningen eller tillämpningen av detta avtal ska lösas genom samråd mellan parterna. De får inte hänskjutas till nationell eller internationell domstol eller annan tredje part för avgörande.

ARTIKEL 13

SLUTBESTÄMMELSER

1. Detta avtal träder i kraft när det har undertecknats av båda parter.

2. Avtalet får ändras efter båda parters skriftliga samtycke. Sådana ändringar träder i kraft när de har undertecknats av båda parter.

3. Avtalet gäller på obestämd tid, om inte någon av parterna på diplomatisk väg skriftligen meddelar den andra parten om sin avsikt att säga upp avtalet. I sådana fall upphör avtalet att gälla sex (6) månader efter den dag då meddelandet om uppsägning lämnades till den andra parten.

4. Alla säkerhetsskyddsklassificerade försvarsrelaterade uppgifter som överförs enligt detta avtal ska fortsätta att skyddas i enlighet med bestämmelserna i detta avtal även om avtalet sägs upp.

5. Parterna ska omedelbart underrätta varandra om alla ändringar i sina nationella lagar och andra författningar som påverkar skyddet av de säkerhetsskyddsklassificerade försvarsrelaterade uppgifter som lämnats ut enligt detta avtal. I sådana fall ska parterna samråda med varandra och överväga att ändra detta avtal. De säkerhetsskyddsklassificerade försvarsrelaterade uppgifterna

ska under tiden fortsätta att vara skyddade i enlighet med detta avtal om inte ursprungsparten skriftligen begär något annat.

SÖ 2012:23

Undertecknat i Stockholm den 15 juni 2012 och i Dublin den 16 juli 2012 i två original på engelska.

Till bekräftelse härav har undertecknade, därtill vederbörligen bemyndigade av sina respektive regeringar, undertecknat detta avtal.

För Konungariket Sveriges regering

För Irlands regering

Nils Cederstierna

Ciaran Murphy

**GENERAL SECURITY ARRANGEMENT BETWEEN
THE GOVERNMENT OF THE KINGDOM OF SWEDEN
AND
THE GOVERNMENT OF IRELAND
ON
THE MUTUAL PROTECTION
OF DEFENCE CLASSIFIED INFORMATION**

INTRODUCTION

The Government of the Kingdom of Sweden and the Government of Ireland, hereinafter referred to as the Participants, have, in the interest of national security and for the purpose of ensuring the protection of Defence Classified Information exchanged between them, decided as follows:

**SECTION 1
DEFINITIONS**

In this Arrangement, the following definitions will be used:

1. **Defence Classified Information:** Defence Information, regardless of its form, that under the laws of either Participant requires protection against loss, unauthorised disclosure or other compromise, and has been so designated.

2. **Originating Participant:** The Participant, including any public or private entities under its jurisdiction, which transfers Defence Classified Information to the other Participant.

3. **Recipient Participant:** The Participant, including any public or private entities under its jurisdiction, which receives Defence Classified Information from the other Participant.

4. **Third Party:** A state, including any public or private entities under its jurisdiction, or an international organisation not a participant to this Arrangement.

5. **Classified Contract:** A contract, which contains or involves Defence Classified Information.

6. **Security Clearance:** A positive determination stemming from a vetting procedure that will ascertain loyalty and trustworthiness as well as other security aspects of an individual or a legal entity in accordance with national laws and regulations.

7. **Need-to-know Principle:** The necessity to have access to Defence Classified Information in order to be able to perform official duties and tasks.

**SECTION 2
SECURITY CLASSIFICATIONS**

1. Defence Classified Information released under this Arrangement will be marked by security classification markings as appropriate under the national laws and regulations of either Participant. Received Defence Classified Information will be granted protection in accordance with the equivalent security classification level, as stated in Paragraph 2.

2. The equivalence of national security classification markings will be as follows:

Defence Authorities	Other Authorities	Defence Authorities
HEMLIG/TOP SECRET	HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	TOP SECRET
HEMLIG/SECRET	HEMLIG	SECRET
HEMLIG/CONFIDENTIAL	–	CONFIDENTIAL
HEMLIG/RESTRICTED	–	RESTRICTED

3. Information from the Kingdom of Sweden bearing the sole marking of “HEMLIG” will be treated as SECRET in Ireland unless otherwise requested by the Originating Participant.

4. The Originating Participant will without delay notify the Recipient Participant of any changes to the security classification of released Defence Classified Information.

SECTION 3 COMPETENT SECURITY AUTHORITIES

1. For the purpose of this Arrangement, the Competent Security Authorities will be:

In the Kingdom of Sweden:

Försvarsmakten

Militära säkerhetstjänsten (National Security Authority for defence matters)

Försvarets materielverk (Designated Security Authority for industrial security matters)

In Ireland:

Department of Defence

2. Each Participant will provide the other Participant with the necessary contact data of their Competent Security Authorities.

SECTION 4 DISCLOSURE AND USE OF DEFENCE CLASSIFIED INFORMATION

1. The Recipient Participant will take all lawful steps to prevent the disclosure or use of Defence Classified Information released, except for the purposes and within limitations stated by the Originating Participant.

2. Subject to its national laws, the Recipient Participant may release Defence Classified Information requested by a Third Party only with the explicit written approval of the Originating Participant.

SECTION 5
ACCESS TO DEFENCE CLASSIFIED INFORMATION

1. Access to Defence Classified Information will be limited, in accordance with the Need-to-Know Principle and the respective Participants' national standards, to Persons:

- a) who hold valid security clearance at the appropriate classification level and
- b) who have been briefed on Defence Classified Information protection.

2. Subject to fulfilment of procedural requirements laid out in national law, the Participants will mutually recognise their respective certificates of Security Clearance.

SECTION 6
PROTECTION OF DEFENCE CLASSIFIED INFORMATION

1. The Originating Participant will:

- a) ensure that transferred Defence Classified Information is marked with an appropriate national security classification marking according to SECTION 2.2;
- b) inform the Recipient Participant of any provisions of release or limitations on the use of the Defence Classified Information, as applicable;
- c) inform the Recipient Participant of any subsequent changes in the security classification of transferred Defence Classified Information.

2. The Recipient Participant will:

- a) afford the equivalent level of security protection to Defence Classified Information as afforded by the Originating Participant;
- b) ensure that security classifications are not altered, except if authorised in writing by the Originating Participant.

SECTION 7
TRANSFER OF DEFENCE CLASSIFIED INFORMATION

1. Defence Classified Information will be transferred between the Participants in accordance with national laws and regulations of the Originating Participant, through diplomatic channels or as otherwise agreed between the Competent Security Authorities.

2. The Participants may agree on separate Communication/Security Arrangements for the purpose of regulating secure communication between them.

SECTION 8
VISITS

1. Visits to facilities where Defence Classified Information is handled or stored will be subject to prior approval by the Competent Security Authorities of the host Participant, unless otherwise agreed.

2. A request for visit will be submitted to the Competent Security Authorities of the host Participant, normally at least one Calendar month prior to the visit, and will include the following:

- a) name of the visitor, date and place of birth, nationality, passport number and a copy of the valid security clearance certificate of the visitor;

- b) specific appointment details of the visitor;
- d) details of the facility and/or person to be visited;
- e) purpose of the visit;
- g) dates and duration of the visit(s).

3. Any Defence Classified Information disclosed or made available to visitors from a Participant will be treated as if transferred to that Participant, and will be protected accordingly. All visitors will comply with the security regulations of the host Participant.

SECTION 9 CLASSIFIED CONTRACTS

1. The Participants will mutually recognise their respective certificates of Facility Security Clearance (hereinafter FSC). Each Competent Security Authority may request that a security inspection is carried out at a facility of the other Participant to ensure continuing compliance with security standards according to national laws and regulations of that Participant.

2. A Classified Contract will contain guidelines on the security requirements and on the classification of each aspect or element of the Classified Contract.

SECTION 10 SECURITY CO-OPERATION for Defence Classified Information

1. In order to achieve and maintain comparable standards of security, the Competent Security Authorities may, on request, provide each other with information about their national security standards, procedures and practices for the protection of Defence Classified Information. In this respect the Competent Security Authorities may conduct mutual visits.

2. The Competent Security Authorities will inform each other of current security risks that may endanger transferred Defence Classified Information, as applicable.

3. On request, the Competent Security Authorities may, within the limits set by their national laws and regulations, assist each other in carrying out security clearance procedures.

4. If either Competent Security Authority suspends or takes action to revoke access to Defence Classified Information which is granted to a national of the other Participant based upon a security clearance, the other Participant will be notified and given the reasons for such an action.

SECTION 11 LOSS, UNAUTHORISED ACCESS TO OR UNAUTHORISED DISCLOSURE OF DEFENCE CLASSIFIED INFORMATION

1. In the event of the loss, unauthorised access to, or unauthorised disclosure of Defence Classified Information, or suspicion thereof, the Competent Security Authority of the Recipient Participant will immediately inform the Competent Security Authority of the Originating Participant in writing.

2. The appropriate authorities of the Recipient Participant (assisted by competent authorities of the Originating Participant, if required) will carry out an immediate investigation of the incident in accordance with their national

laws and regulations. The Recipient Participant will without delay inform the Originating Participant about the circumstances of the incident, possible security implications, measures adopted for the mitigation of the loss or damage and the outcome of the investigation.

SECTION 12 INTERPRETATION AND DISPUTES

1. This Arrangement is intended to be in conformity with the national laws of the Participants and with international law. In case of conflict, the applicable national law will prevail.

2. Any dispute regarding the interpretation or application of this Arrangement will be resolved by consultation between the Participants and will not be referred to any national or international tribunal or third party for settlement.

SECTION 13 FINAL PROVISIONS

1. This Arrangement will come into effect on the day of the last signature.

2. This Arrangement may be amended with the mutual written consent of both Participants. Such amendments will come into effect on the day of the last signature.

3. This Arrangement will remain in force for an indefinite period of time, unless either Participant notifies the other in writing through diplomatic channels of its intention to terminate the Arrangement. In this case the Arrangement will expire after six (6) months following the day on which the termination notice was served on the other Participant.

4. Notwithstanding the termination of this Arrangement, all Defence Classified Information transferred under this Arrangement will continue to be protected in accordance with the provisions set out herein.

5. The Participants will promptly notify each other of any changes to their national laws and regulations that affect the protection of Defence Classified Information released under this Arrangement. In such case, the Participants will consult to consider possible amendments to this Arrangement. In the meantime, the Defence Classified Information will continue to be protected as described herein, unless otherwise requested by the Originating Participant in writing.

Signed in Stockholm on 15 June 2012 and in Dublin on 16 July 2012 in two original copies, each in English.

In witness of which the undersigned, duly authorised to this effect by their respective governments, have signed this Arrangement.

For the Government of the Kingdom
of Sweden

Nils Cederstierna

For the Government of Ireland

Ciaran Murphy