

Arrangement de mise en œuvre

**entre le Département fédéral de la défense, de la protection
de la population et des sports de la Confédération suisse
et l'Agence européenne de défense concernant la protection
des informations classifiées**

Conclu le 23 juin 2022

Entré en vigueur le 23 juin 2022

(Etat le 23 juin 2022)

*Le Département fédéral de la défense, de la protection de la population et des sports
de la Confédération suisse
et*

l'Agence européenne de défense,

ci-après dénommés collectivement «les parties» et individuellement «la partie»,

considérant l'art. 10 du cadre de coopération entre les parties, signé le 16 mars 2012,
qui prévoit que toute communication et tout échange d'informations classifiées
doivent être conformes à l'accord du 28 avril 2008 entre la Confédération suisse et
l'Union européenne sur les procédures de sécurité pour l'échange d'informations
classifiées¹ (ci-après dénommé «accord sur les procédures de sécurité»),

notant que cet article doit être précisé dans un arrangement de mise en œuvre
(ci-après dénommé «arrangement») afin d'établir des dispositions au niveau opérationnel,

souhaitant assurer la protection des informations classifiées détenues et échangées
entre les parties, et

notant que les dispositions du présent arrangement sont conformes à l'accord sur les
procédures de sécurité et constituent un cadre adéquat pour l'échange d'informations
classifiées conformément aux règles de sécurité définies dans la décision du Conseil
2013/488/EU², lesquelles s'appliquent à l'AED en vertu de l'art. 32 de la décision
du Conseil (PESC) 2015/1835³.

sont convenus des dispositions suivantes:

Art. 1 Autorités de sécurité compétentes

1. Les autorités de sécurité compétentes responsables de l'application du présent
arrangement sont:

RO 2022 402

¹ RS 0.514.126.81

² JO L 274 du 15.10.2013, p. 1

³ JO L 266 du 13.10.2015, p. 55

- (a) *pour le Département fédéral de la défense, de la protection de la population et des sports (DDPS):*
le domaine «Digitalisation et cybersécurité du DDPS» (DCS DDPS);
 - (b) *pour l'Agence européenne de défense (AED):*
la division «Corporate Services», et
le domaine «Security and Infrastructure».
2. Chaque partie informe l'autre partie de tout changement affectant son autorité de sécurité compétente.
3. Chaque partie prend les mesures appropriées pour coordonner avec l'autre partie toutes les exigences et procédures relatives à la mise en œuvre du présent arrangement.

Art. 2 Système de classification et identification de l'entité d'origine

1. Toutes les informations classifiées communiquées par une partie à l'autre partie portent une marque indiquant le niveau de classification de sécurité conforme aux réglementations de sécurité appliquées par la partie dont émane l'information.
2. Les marques indiquant le niveau de classification de sécurité ci-après sont considérées comme équivalentes:

AED	SUISSE
RESTREINT UE/EU RESTRICTED	INTERN/INTERNE/AD USO INTERNO
CONFIDENTIEL UE/EU CONFIDENTIAL	VERTRAULICH/CONFIDENTIEL/ CONFIDENZIALE
SECRET UE/EU SECRET	GEHEIM/SECRET/SEGRETO

3. Pour identifier l'entité d'origine des informations et pour définir notamment ses droits, les informations classifiées provenant de l'AED portent la mention «AED» à côté ou en dessous de chaque marque indiquant le niveau de classification de sécurité UE.
4. En plus des marques indiquant le niveau de classification de sécurité visées à l'art. 2, al. 2, ci-dessus, les informations classifiées produites par une partie et communiquées à l'autre partie contiennent une déclaration de communicabilité explicite telle que:

SECRET UE/EU SECRET
RELEASABLE TO SWITZERLAND
GEHEIM/SECRET/SEGRETO
RELEASABLE TO EDA

D'autres limitations d'accès ou de distribution peuvent être ajoutées à la déclaration de communicabilité si l'entité d'origine le juge nécessaire.

Art. 3 Habilitation de sécurité du personnel et autorisation d'accès

1. L'accès aux informations classifiées est réservé aux personnes ayant besoin d'en connaître. En outre, les personnes dont la fonction requiert l'accès aux informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou VERTRAULICH/CONFIDENTIEL/CONFIDENZIALE, ou SECRET UE/EU SECRET ou GEHEIM/SECRET/SEGRETO doivent, en plus d'avoir besoin d'en connaître, détenir une habilitation de sécurité du personnel (PSC) valable délivrée conformément aux réglementations de sécurité des parties.

2. Avant de se voir accorder l'accès à des informations classifiées, toute personne ayant besoin d'y accéder doit être informée de la réglementation de sécurité relative à la classification des informations concernées. Ces personnes confirment par écrit qu'elles ont été informées de la réglementation de sécurité applicable et que toute violation de cette dernière peut entraîner des mesures disciplinaires ou d'éventuelles poursuites judiciaires conformément aux lois et réglementations en vigueur.

Art. 4 Protection des informations classifiées

1. Le présent arrangement s'applique aux informations classifiées communiquées ou échangées entre les parties.

2. Chaque partie veille à la protection et à la sauvegarde des informations classifiées visées par le présent arrangement qui sont communiquées par l'autre partie ou échangées avec elle.

3. La partie destinataire veille à la protection et à la sauvegarde des informations classifiées de l'autre partie, conformément aux dispositions établies dans sa propre réglementation régissant la sécurité des informations classifiées à un niveau équivalent au sens de l'art. 2, al. 2, du présent arrangement.

4. Chaque partie s'abstient d'exploiter les informations classifiées échangées dans le cadre du présent arrangement à des fins autres que celles qui ont été définies par l'entité d'origine et que celles pour lesquelles les informations ont été communiquées ou échangées.

5. Chaque partie s'abstient de communiquer les informations classifiées visées par le présent arrangement à des tiers sans le consentement écrit préalable de l'entité d'origine.

Art. 5 Bureaux d'ordre et contrôle des informations classifiées

1. Un système de bureaux d'ordre est mis en place pour la réception, la distribution, le contrôle et le stockage des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL ou VERTRAULICH/CONFIDENTIEL/CONFIDENZIALE ou plus haut, comme défini par les réglementations de chaque partie.

2. Les parties s'informent mutuellement des bureaux d'ordre autorisés à recevoir et à traiter les informations classifiées échangées dans le cadre du présent arrangement et veillent à ce que ces bureaux d'ordre offrent un niveau de protection équivalent.

3. Les bureaux d'ordre sont responsables:

- (a) de la distribution et du contrôle des informations classifiées;
- (b) du stockage des informations classifiées, et,
- (c) de l'élimination définitive, du déclassément et/ou de la déclassification conformément aux instructions de l'entité d'origine, ainsi que de la conservation des certificats de destruction des informations classifiées CONFIDENTIEL UE/UE CONFIDENTIAL et plus haut de l'AED et des procès-verbaux de destruction des informations classifiées VERTRAULICH/CONFIDENTIEL/CONFIDENZIALE et plus haut de la Suisse.

4. Les autorités de sécurité compétentes des parties sont responsables de l'ouverture et de la supervision des bureaux d'ordre au sein de leurs administrations respectives. Elles s'informent mutuellement de l'ouverture ou de la fermeture de bureaux d'ordre stockant les informations classifiées de chaque partie.

Art. 6 Transmission des informations classifiées entre les parties

1. Les informations classifiées RESTREINT UE/EU RESTRICTED ou INTERN/INTERNE/AD USO INTERNO peuvent être transmises entre les parties par transport dans un bagage à main, services postaux, services de messagerie commerciale ou par voie électronique en utilisant des produits de cryptage convenus entre les autorités de sécurité compétentes visées à l'art. 1 ci-dessus.

2. Les informations classifiées CONFIDENTIEL UE/UE CONFIDENTIAL ou VERTRAULICH/CONFIDENTIEL/CONFIDENZIALE peuvent être transmises entre les parties par valise diplomatique, transport dans un bagage à main par une personne ayant reçu une habilitation de sécurité appropriée et munie d'un ordre de mission de messenger délivré par la partie qui transmet les informations, ou par un service de messagerie commerciale approuvé conformément à la réglementation de sécurité de la partie qui transmet les informations.

3. Les informations classifiées CONFIDENTIEL UE/UE CONFIDENTIAL ou VERTRAULICH/CONFIDENTIEL/CONFIDENZIALE ou plus haut ne sont pas transmises entre les parties par voie électronique, sauf accord mutuel des parties et sous réserve de la mise en place de mesures spécifiques de sécurité des informations et des communications ainsi que de l'utilisation de produits de cryptage convenus entre les autorités de sécurité compétentes.

4. La transmission des informations classifiées SECRET UE/EU SECRET ou GEHEIM/SECRET/SEGRETO, au moyen de coursiers désignés, est réglementée au cas par cas.

Art. 7 Visites

1. Aux fins du présent arrangement, et sans préjudice des visites d'évaluation, chaque partie autorise des représentants de l'autre partie ou de ses entrepreneurs à visiter ses établissements, sous réserve du respect des règles de sécurité applicables de la partie hôte.

2. Pour les visites nécessitant l'accès à des informations classifiées CONFIDENTIEL UE/UE CONFIDENTIAL ou VERTRAULICH/CONFIDENTIEL/CONFIDENZIALE ou plus haut, ou durant lesquelles les visiteurs peuvent avoir accès à de telles informations, une demande de visite est soumise à la partie hôte ou à d'autres autorités de sécurité compétentes désignées par la partie hôte, au moyen de formulaires de demande de visite.

Art. 8 Contrats classifiés

1. Les informations classifiées reçues de l'autre partie ne peuvent être communiquées à un entrepreneur ou à un entrepreneur potentiel qu'avec le consentement écrit préalable de la partie qui transmet les informations et lorsqu'un accord ou un arrangement de sécurité a été conclu entre la partie qui transmet les informations et l'État dans lequel l'entrepreneur est enregistré, conformément aux règles de sécurité de la partie qui transmet les informations.

2. Avant de communiquer des informations classifiées CONFIDENTIEL UE/UE CONFIDENTIAL ou VERTRAULICH/CONFIDENTIEL/CONFIDENZIALE ou plus haut, à un entrepreneur ou à un entrepreneur potentiel, la partie destinataire s'assure, conformément aux réglementations en vigueur, que l'entrepreneur ou l'entrepreneur potentiel détient une habilitation de sécurité d'établissement appropriée.

3. Lors de l'attribution d'un contrat visé par le présent arrangement, la partie destinataire notifie la partie qui transmet les informations que le contrat a été attribué. Les exigences de sécurité auxquelles le contrat doit satisfaire sont décrites dans une annexe de sécurité ([Security Aspects Letter (SAL) ou Programme/Project Security Instructions (PSI)]).

Art. 9 Atteintes à la sécurité, perte ou compromission d'informations classifiées

1. Lorsqu'il est avéré ou qu'il y a raisonnablement lieu de suspecter que des informations classifiées reçues de l'autre partie ont été compromises ou perdues, la partie sur le territoire de laquelle l'incident s'est produit doit:

- (a) fournir aussi rapidement que possible à la partie qui transmet les informations un rapport ou une communication initiale indiquant qu'une compromission ou une perte d'informations classifiées a eu lieu;
- (b) mener une enquête approfondie pour établir les faits entourant l'incident;
- (c) fournir à la partie qui transmet les informations un rapport d'enquête écrit et complet, contenant une description détaillée des circonstances ainsi que les conclusions de l'enquête et les mesures engagées ou à engager pour éviter qu'une telle situation ne se reproduise.

2. Les rapports susmentionnés sont remis aux autorités de sécurité compétentes visées à l'art. 1.

3. Toute atteinte à la sécurité, avérée ou suspectée, commise par une personne peut donner lieu à des mesures disciplinaires ou à d'éventuelles poursuites judiciaires conformément aux lois et réglementations en vigueur.

Art. 10 Liaison et visites d'évaluation

1. Les autorités de sécurité compétentes maintiennent une liaison constante afin de superviser la communication et l'échange d'informations classifiées entre les parties. Elles se réunissent à des dates fixées d'un commun accord pour examiner des questions d'intérêt commun et évaluer la mise en œuvre du présent arrangement.

2. Le Bureau de la sécurité de l'AED et le domaine Digitalisation et cybersécurité du DDPS facilitent la conduite de visites d'évaluation mutuelles au sens du ch. 9 de l'annexe VI à la décision du Conseil 2013/488/EU, afin de vérifier que les informations classifiées produites par les parties sont correctement traitées et protégées. Ces visites font l'objet d'un accord préalable entre les parties.

Art. 11 Dispositions finales, révision et modification

1. Le présent arrangement entre en vigueur à la date de la dernière signature.

2. Le présent arrangement peut être revu à la demande de l'une ou l'autre partie. Toute modification doit faire l'objet d'un accord écrit entre les parties.

3. Chaque partie peut résilier le présent arrangement par notification écrite adressée à l'autre partie, en respectant un délai de préavis de six mois. En cas de résiliation, toute information classifiée déjà échangée ou produite dans le cadre du présent arrangement est traitée conformément aux dispositions du présent arrangement aussi longtemps que nécessaire pour la protection des informations classifiées.

4. Les différends entre les parties touchant l'interprétation ou l'application du présent arrangement sont réglés par voie de négociation entre les parties, au niveau le plus bas possible, et ne sont soumis ni à un tribunal national ou international ni à des tiers pour règlement.

Signé à Bruxelles, le 23 juin 2022, en deux exemplaires originaux, chacun en langue anglaise et allemande. En cas de divergence quant à leur interprétation, le texte en langue anglaise fait foi.

Pour
le Département fédéral de la défense,
de la protection de la population et des sports
de la Confédération suisse:

Roger Michlig

Pour
l'Agence européenne de défense:

Olli Ruutu