



Conseil de l'Union européenne
Secrétariat général

Bruxelles, le 25 mars 2022

CM 2347/22

CYBER
COPEN
COPS
COSI
DATAPROTECT
IND
JAI
JAIEX
POLMIL
RELEX
TELECOM

COMMUNICATION

CONVOCATION ET ORDRE DU JOUR PROVISOIRE

Correspondant: cyber@consilium.europa.eu
Tél./Fax: +32 2 281 3607

Objet: Groupe Horizontal sur les Questions Cyber

Date: 29 mars 2022
Heure: 9:30
Lieu: CONSEIL
BÂTIMENT JUSTUS LIPSIUS
Rue de la Loi 175, 1048 BRUXELLES

Veillez noter syp que la réunion commence à 9h30.

Format: 1+1 pour les délégations, 2+2 pour la présidence, la Commission et le SGC

Session du matin – 9h30

1. Adoption de l'ordre du jour

2. **Boîte à outils cyber-diplomatique¹ (CONFIDENTIEL-UE)***
 - Présentation du SEAE
 - Présentation de la Commission
 - Discussion
3. **Régime de sanctions cyber de l'UE (RESTREINT-UE)**
 - Présentation du SEAE
 - Discussion
4. **Convention de l'ONU sur la cybercriminalité**
 - Présentation de la REV1 par la Présidence
 - Présentation par la Commission
 - Discussion
5. **Discussion entre l'Union européenne et les États-Unis au sujet des rançongiciels**
 - Présentation de la Commission
 - Discussion

Session de l'après-midi – 14h30

6. **Proposition de règlement établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l'Union²**
 - Présentation de la proposition et de l'analyse d'impact par la Commission
 - Discussion7474/22 + ADD 1 + ADD 2 + ADD 3
7. **Projet de conclusions du Conseil sur le rapport spécial de la Cour des comptes européenne - « Déploiement des réseaux 5G au sein de l'UE : des retards et des questions de sécurité encore sans réponse »**
 - Présentation du projet révisé
 - Discussion
8. **Directive NIS2**
 - Retour sur la réunion technique du 25 avril 2022
 - Présentation du calendrier prévisionnel en vue du trilogue politique du 25 avril 2022
 - Suite de la discussion sur la base du tableau 4 colonnes (à partir de l'article 6) 7287/22 (à diffuser)
9. **Points divers**

NB: Les documents du Conseil sont disponibles sur le Portail des délégués.

* * *

¹ Ce point sera discuté en présence de CERT-EU.

² Ce point sera discuté en présence de CERT-EU.

* Cette réunion va traiter des informations classifiées au niveau : "**CONFIDENTIEL UE/EU CONFIDENTIAL**".

Conformément aux règles de sécurité du Conseil, tous les délégués présents lors de l'examen de ces points, doivent posséder une **habilitation de sécurité personnelle (HSP) valide, au minimum du niveau "CONFIDENTIEL UE/EU CONFIDENTIAL" afin d'accéder à la salle de réunion lorsque les points seront discutés.**

Les délégués sont priés de noter que, conformément au règlement de sécurité du Conseil, seules les personnes titulaires d'une HSP valide et ayant le besoin d'en connaître, peuvent participer aux réunions quand ces informations classifiées doivent être discutées.

Les délégations sont priées de transmettre la liste des participants **au plus tard le 25 mars 2022 à 18:00 heures** à l'adresse courriel suivante wp-cyber@consilium.europa.eu afin de permettre à la direction Prévention et Sécurité de s'assurer que tous les participants disposent d'une HSP valide pour la réunion.

Vous devez envoyer les informations suivantes pour chaque délégué participant à la réunion : nom(s) de famille, prénom, nationalité, date de naissance, le nom de l'organisation/institution d'appartenance du délégué.

Sur la base de ces informations, si la direction Prévention et Sécurité ne dispose d'aucune information sur l'HSP des délégués, nous vous en informerons et votre autorité nationale de sécurité ou toute autre autorité nationale compétente ou l'officier de sécurité de votre organisation devra envoyer un certificat de l'HSP valide à l'attention de l'équipe en charge de la gestion des habilitations du secrétariat général du Conseil à l'adresse courriel suivante: security.clearances@consilium.europa.eu

1. **Veillez noter que les certificats envoyés par les délégués eux-mêmes ne seront pas acceptés.**
2. Veillez indiquer la référence de la réunion dans le sujet pour un traitement plus rapide.
3. Il est dans l'intérêt des participants de s'assurer que leur habilitation de sécurité personnel n'a pas expiré.

Aucune admission à la discussion d'un point classifié ne sera accordée aux délégués pour lesquels la direction Prévention et Sécurité n'a aucun certificat d'habilitation de sécurité personnelle enregistré ou qui ne peut pas présenter un certificat original et valide pour accéder à des informations classifiées de l'UE, délivré par leurs autorités nationales de sécurité ou par d'autres autorités nationales compétentes ou l'officier de sécurité de leur organisation.

Lors de la discussion des points *CONFIDENTIEL UE/EU CONFIDENTIAL*, **tous les appareils électroniques doivent être éteints.** S'ils ne peuvent pas être facilement désactivés, ils ne peuvent pas être conservés dans la salle de réunion.