Reply of the European Commission to the proposal of the European Ombudsman for a solution on the European Commission's implicit refusal to give public access to minutes of meetings of the Network and Information Systems Cooperation Group - Complaint by Mr [redacted], ref. 228/2024/NH

I. BACKGROUND/SUMMARY OF THE FACTS/HISTORY

On 26 July 2023, the applicant submitted a request[1] for access to documents under Regulation (EC) No 1049/2001 regarding public access to European Parliament, Council and Commission documents (hereafter 'Regulation (EC) No 1049/2001')[2].

In his application, handled by the Directorate-General for Communication Networks, Content and Technology (hereafter 'DG CNECT'), the applicant requested access to:

1. meeting agendas, minutes and reports of the Network and Information Systems (NIS) Cooperation Group established by the NIS Directive;[3]
2. the guidelines provided under Article 4 (3) of NIS 2 Directive[4] and, as the case may be, any related observations of the Cooperation Group and ENISA;
3. the guidelines mentioned in recital 20 of NIS 2 Directive;
4. the guidance mentioned in recital 21 of the NIS 2 Directive.

In its initial reply of 28 September 2023, DG CNECT informed the applicant that the meeting agendas are publicly available on the Commission webpage[5]. As regards the minutes of the meetings, DG CNECT identified 24 documents falling under the scope of the applicant's request. It refused access to the documents based on the exception laid down in the first indent (protection of the public interest as regards public security) of Article 4(1)(a) of Regulation (EC) No 1049/2001. As regards points 2, 3 and 4 of the applicant's request, DG CNECT informed the applicant that it did not hold any document corresponding to his request.

On 17 October 2023, the applicant submitted a confirmatory application asking for the revisions of the position taken by DG CNECT at initial stage. Following a review of the reply given by DG CNECT, by the confirmatory decision[6] adopted on 19 August 2024, the Commission identified 27 documents, corresponding to the minutes of the meetings of the NIS Cooperation Group, from the first to the 27th meeting.

The Commission granted partial access to 27 documents with redactions based on the exceptions laid down in Article 4(1)(a) (protection of the public interest as regards public

---

1 Registered with reference EASE 2023/4388.
2 OJ L 145 of 31.5.2001, p. 43.
3 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1, Directive - 2016/1148 - EN - EUR-Lex (europa.eu).
4 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), OJ L 333, 27.12.2022, p. 80, Directive - 2022/2555 - EN - EUR-Lex (europa.eu).
5 https://digital-strategy.ec.europa.eu/en/library/nis-cooperation-group-meetings-agendas
6 C(2024)5942.

security) and Article 4(1)(b) (protection of privacy and the integrity of the individual) of Regulation (EC) No 1049/2001.

Furthermore, the Commission indicated the links to the webpages where the Commission Guidelines on the application of Article 3(4) of NIS 2 Directive and the Commission Guidelines on the application of Article 4 (1) and (2) of NIS 2 Directive were publicly available[7].

As regards the minutes of the 28th meeting of the NIS Cooperation Group, the latter took place on 27 and 28 September 2023. Since the initial request was submitted on 26 July 2023, the Commission informed the applicant that the minutes of the 28th meeting fall outside the scope of the request.

II. THE COMPLAINT TO THE EUROPEAN OMBUDSMAN

The applicant submitted a complaint to the Ombudsman for failure to reply within the statutory deadline and for refusing to disclose the documents. In addition, the complainant argued that the Commission did not identify all documents falling within the scope of his request. In particular, he contends that the Commission should have identified (and granted access to) the minutes of the 16th, 17th, 27th and 28th meeting, as these meetings appear on the Commission's website listing the agendas of all NIS Cooperation Group meetings.

III. THE EUROPEAN OMBUDSMAN'S INQUIRY AND RECOMMENDATION

The Ombudsman opened an inquiry into this complaint and, in light of the delay taken to adopt a decision, asked the Commission to inspect the documents at issue.

In its proposal, the Ombudsman took the view that the Commission should have granted wide partial access to the documents.

The Ombudsman considered that the Commission, while enjoying a wide margin of discretion when deciding on what the protection of public security calls for in terms of disclosure of documents, was still required to demonstrate a risk to public security that was reasonably foreseeable and not purely hypothetical.

Following the inspection carried out by the Ombudsman inquiry team, the Ombudsman took the view that the documents, 'to a very large extent, do not seem to contain any sensitive content: the minutes are drafted in rather general terms and do not provide any sensitive details about concrete operational work by NIS authorities. Sensitive content or presentations appear to have been shared with members of the NIS Cooperation Group through a secure platform […]'.

[7] https://digital-strategy.ec.europa.eu/en/library/commission-guidelines-application-article-34-directive-eu-20222555-nis-2-directive and https://digital-strategy.ec.europa.eu/en/library/commission-guidelines-application-article-4-1-and-2-directive-eu-20222555-nis-2-directive

However, the Ombudsman noted that, in several documents[8], certain discussion points could reveal operational details. They relate among others to 'the war in Ukraine, the way Member States apply sanctions and penalties, activities by specific third countries, scenarios concerning large-scale attacks on the energy sector or Member States' presentations about recent major cyber-attacks'.

In addition, the Ombudsman took the view that 'a large part of the discussions concern updates from the Member States on their transposition of the first NIS Directive, or positions on the review of the directive, or updates on the transposition of the NIS2 Directive'. The Ombudsman considered that, given the passage of time, 'it is difficult to see how these aspects can be considered sensitive, and thus covered by the public security exception'.

As regards any personal data in the documents, the Ombudsman noted that they could be easily redacted.

Furthermore, the Ombudsman found that the Commission should have indeed identified three of the additional documents indicated by the complainant (minutes of the 16th, 17th and 27th meeting), and granted wide partial access to them, for the same reasons explained above. As regards the minutes of the 28th meeting, the Ombudsman considered that this document was finalised after the complainant made his request and therefore fell outside of its scope.

The Ombudsman noted that the Commission Implementing Decision (EU) 2017/179[9] set out explicitly that the Group's discussions shall not be open to the public. However, in light of Article 10(1)[10] and Article 10(3)[11] of the same Implementing Decision, the Ombudsman considered that the Commission should base its assessment of the request for public access on the provisions of Regulation (EC) No 1049/2001.

In light of the above, the Ombudsman proposed that the Commission should reconsider its position on the complainant's request, with a view to granting the widest possible access to the documents, including the three additional documents that were not identified at initial stage.

IV. THE EUROPEAN COMMISSION'S REPLY TO THE RECOMMENDATION OF THE EUROPEAN OMBUDSMAN

In its confirmatory decision, the Commission identified 27 minutes of the NIS Cooperation Group meetings, in line with the Ombudsman opinion on the identification of documents.

---

8 Documents numbered 9, 13, 17, 20 and 21.

9 Commission Implementing Decision (EU) 2017/179 of 1 February 2017 laying down procedural arrangements necessary for the functioning of the Cooperation Group pursuant to Article 11(5) of the Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union, C/2017/0438, OJ L 28, 2.2.2017, p. 73–77.

10 Requests addressed to the Group for access to the documents concerning its activities shall be handled by the Commission in accordance with Regulation (EC) No 1049/2001.

11 Documents submitted to members of the Group, representatives of third parties and experts shall not be disclosed to the public, unless access is granted to those documents pursuant to paragraph 1 or they are otherwise made public by the Commission.

The Commission granted partial access to the 27 documents, considering that parts of the documents were covered by the public security exception laid down in Article 4(1)(a) of Regulation (EC) No 1049/2001. In addition, personal data have been protected under the exception laid down in Article 4(1)(b) (protection of privacy and the integrity of the individual) of Regulation (EC) No 1049/2001.

The Ombudsman recommended the Commission to grant the widest possible access to the documents. The Commission considers that, by its confirmatory decision C(2024)5942, it fulfilled the requirement on the widest possible access to the documents concerned, taking into account the risks for the public security that the disclosure would trigger, as explained in detail in the decision. As regards the motivation, the Commission has, to the proper standard of reasoning, explained how access to the redacted parts of the documents could specifically and actually undermine the interest protected by the exception laid down in Article 4(1)(a) of Regulation (EC) No 1049/2001. The Commission also demonstrated that the risk of that interest being undermined was reasonably foreseeable and not purely hypothetical.

The Commission disagrees with some of the statements made by the Ombudsman in its Proposal.

The Commission would like first to underline that the documents requested by the applicant are the minutes of the meetings of the Network and Information Systems Cooperation Group ('NIS Cooperation Group').

As explained in the decision, the NIS Cooperation Group was established by the NIS Directive[12] to ensure cooperation and exchange of information between Member States. In the context of increasing cyber threat and societal dependence on network and information systems, the objective of the directive is to improve the resilience and incident response capacities of public and private entities, competent authorities, and the EU as a whole in the field of cybersecurity and critical infrastructure protection. The directive aims to strengthen the European cooperation both at political (through the NIS Cooperation Group) and at technical level (within the framework of the Computer Security Incident Response Team (CSIRTs))[13], and to improve crisis management (through the creation of the European cyber crisis liaison organisation network (EU-CyCLONe)). In addition to this legal framework, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented a new EU Cybersecurity Strategy[14] at the end of 2020. The strategy focuses on building collective capabilities to respond to major cyber-attacks and working with partners around the world to ensure international security and stability in cyberspace.

Article 14 of Directive (EU) 2022/2555 (NIS2) specifies the tasks of the NIS Cooperation Group. It also provides that 'Member States shall ensure effective, efficient and secure

[12] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), OJ L 333, 27.12.2022. This Directive is the successor to the NIS 1 Directive.

[13] Computer Security Incident Response Team: https://csirtsnetwork.eu

[14] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

cooperation of their representatives in the Cooperation Group'. The NIS Cooperation Group operates in accordance with the Commission Implementing Decision of 1 February 2017.

The NIS Cooperation Group is composed of representatives of the Member States, the Commission, and the European Union Agency for Network and Information Security (ENISA). The secretariat of the group is provided by the European Commission[15]. The Commission publishes the agendas of all NIS Cooperation Group meetings[16]. As a general rule, the group meets four times a year.

The topics discussed at these meetings and recorded in the relevant documents relate to the tasks assigned by the NIS2 Directive.

The Ombudsman is of the view that most of the documents do not seem to contain any sensitive content.

As explained in the decision, parts of the documents contain opinions and views of Member States on deliverables (e.g. 5G cybersecurity), updates on all work streams, as well as other current and future actions and discussions at national and cross-border level. They also contain information on incidents and other actions taking place in the Member States. They reflect discussions on cybersecurity on specific related issues, such as the 2019 European elections, the implementation of the Commission recommendations, the state of play and updates of the different actions, including the implementation of the Group's recommendations, the work concerning the CSIRTs network and the EU Cybersecurity Strategy.

The Commission takes the view that public disclosure of these parts of the documents would undermine the protection of public security as it would provide the wider public, including malicious individuals or groups, with relevant information on the fight against cyberattacks. The Commission considers that this would make Member States and Europe fully vulnerable to security incidents and threats.

The Commission agrees with the Ombudsman that certain information in the documents, at first sight, might appear as harmless, in particular from the perspective of normal users. However, the Commission would like to underline that this information put in a certain context could provide valuable information to the outside world, including possible cyber criminals. The Commission has made an individual assessment of all the documents and identified all the information whose disclosure would pose a risk for the public security. This information has been redacted. This includes the details on the platform used for exchanging information by the members of the NIS Cooperation Group, which appears in its proposal for a solution, and which the Commission would like to ask the Ombudsman to keep confidential. Although it is clear that additional relevant information has been exchanged among the participants in relation to the topics discussed in the meetings, the concrete modalities for sharing sensitive information among the participants should remain protected. Taking into

[15] Article 14 (3) of the NIS 2 Directive.
[16] https://digital-strategy.ec.europa.eu/en/library/nis-cooperation-group-meetings-agendas

account the EU efforts to prevent cybercrime as described above, the Commission considers that preventing attacks in the very area of the fight against cyberattacks is a priority.

As regards the application of Regulation (EC) No 1049/2001 in the present case, Article 10 of the Commission Implementing Decision (EU) 2017/179[17] laying down the procedural arrangements necessary for the functioning of the NIS Cooperation Group, establishes that the requests for access to documents concerning the activities of the NIS Cooperation Group will be handled in accordance with Regulation (EC) No 1049/2001. However, the same legal basis sets out the peculiar and specific framework under which the NIS Cooperation Group runs its activities. It provides from the outset the fact that the Group's discussions will not be open to the public. The Commission takes the view that, in the assessment of the request, it cannot ignore the sensitive character of the activities reflected in the documents and the purposes of the cooperation in the field.

It should be recalled that the objective of the NIS Cooperation Group, as clarified by the NIS2 Directive and Implementing Decision, is to support and facilitate strategic cooperation and the exchange of information, and to enhance trust between Member States. The overall mission of the Group could not be achieved in the absence of trust and confidence among the members of the Cooperation Group. Strategic cooperation between Member States and the sharing of information, experience and best practices related to the security of network and information systems are essential to effectively address the challenges posed by incidents and security risks of those systems across the Union.

The NIS Cooperation Group works closely with Member States to enhance security in all sectors and achieve a high level of protection against cybersecurity incidents that may have a significant impact on Europe’s economy and society. Due to the European dimension of this objective, the Group works in close cooperation and mutual trust with the other members of the group and national authorities to ensure cross-border cooperation. The Union’s public security is, by its very nature, intrinsically linked to the maintenance of a high common level of cybersecurity across the Union.

As cybersecurity cannot be achieved without the cooperation of Member States’ authorities, the Commission considers that the disclosure of the discussions reproduced in the requested documents would jeopardise trust and cooperation in the field of cybersecurity. The fact that some documents date from 2017 does not change the level of risk if the documents were disclosed, as they are closely linked to the current discussions and present actions. The risk to the integrity of the European cybersecurity architecture is still real and non-hypothetical. Moreover, the Commission considers that the chilling effect of the full disclosure of the minutes should not be underestimated since this would undermine the good cooperation

[17] Commission Implementing Decision (EU) 2017/179 of 1 February 2017 laying down procedural arrangements necessary for the functioning of the Cooperation Group pursuant to Article 11(5) of the Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union, C/2017/0438, OJ L 28, 2.2.2017, p. 73–77.

between Member States and other participants in the meetings, as well as the trust established within the NIS Cooperation Group.

As explained in the decision, the disclosure of the redacted parts in the documents would give an overall picture of risks, vulnerabilities and risk mitigation measures for the Union and could reveal potential gaps in existing mitigation measures. Full disclosure of the requested documents would also affect the ability of network operators and public authorities in the Member States to effectively protect their networks against cybersecurity threats. This could have negative consequences for the security of data and the security of present and future IT systems and entail potential risks to the security of society as a whole.

In addition, the Ombudsman assessment is that the Member States updates on their transposition of the first NIS Directive or their position on the review and the transposition of the NIS2 Directive are not of sensitive nature and are not covered by the public security exception. The Commission cannot agree with the Ombudsman on this point.

Parts of the documents that have been redacted concern the state of play of the transposition of the NIS and NIS 2 Directive into national legislation. While the transposition of the NIS 2 Directive is still ongoing, the transposition of the NIS Directive has been finalised. However, the relevant parts concern the various actions taken by the Member States in that regard, or options which have not been adopted. Disclosure of these parts of the documents would have a negative impact on public security as regards the actions taken at national level. The passage of time does not change the level of the risk since the actions described are still most relevant for the fight against cybercrime.

Consequently, such information must be also protected under the exception relating to the protection of the public interest as regards public security.

V. CONCLUSIONS

For the reasons set out above, the Commission considers that the widest possible access has been granted to the documents requested, including the three additional documents that were not identified at initial stage.

For the Commission
Věra JOUROVÁ
Vice-President

Réponse de la Commission européenne à la proposition de solution de la Médiatrice européenne concernant le refus implicite de la Commission européenne d'accorder au public l'accès aux procès-verbaux des réunions du groupe de coopération pour la sécurité des réseaux et des systèmes d'information –
Plainte de M. [redacted], réf. 228/2024/NH

I. CONTEXTE/RÉSUMÉ DES FAITS/HISTORIQUE

Le 26 juillet 2023, le demandeur a introduit une demande[1] d'accès à des documents en vertu du règlement (CE) nº 1049/2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission [ci-après le «règlement (CE) nº 1049/2001»][2].

Dans sa demande, traitée par la direction générale des réseaux de communication, du contenu et des technologies (ci-après la «DG CNECT»), le demandeur sollicitait l'accès:

1. aux ordres du jour, procès-verbaux et comptes rendus des réunions du groupe de coopération pour la sécurité des réseaux et des systèmes d'information (SRI) institué par la directive SRI[3];
2. aux lignes directrices prévues à l'article 4, paragraphe 3, de la directive SRI 2[4] et, le cas échéant, à toute observation y afférente du groupe de coopération et de l'ENISA;
3. aux lignes directrices mentionnées au considérant 20 de la directive SRI 2;
4. aux orientations mentionnées au considérant 21 de la directive SRI 2.

Dans sa réponse initiale du 28 septembre 2023, la DG CNECT a informé le demandeur que les ordres du jour des réunions étaient accessibles au public sur la page web de la Commission[5]. En ce qui concerne les procès-verbaux des réunions, la DG CNECT a recensé 24 documents correspondant à l'objet de la demande du demandeur. Elle a refusé l'accès à ces documents sur la base de l'exception prévue au premier tiret (protection de l'intérêt public en ce qui concerne la sécurité publique) de l'article 4, paragraphe 1, point a), du règlement (CE) nº 1049/2001. S'agissant des points 2, 3 et 4 de la demande, la DG CNECT a informé le demandeur qu'elle ne détenait aucun document correspondant à sa demande.

Le 17 octobre 2023, le demandeur a présenté une demande confirmative sollicitant une révision de la position adoptée par la DG CNECT au stade initial. Après avoir examiné la réponse donnée par la DG CNECT, la Commission a, dans sa décision confirmative[6] adoptée le 19 août 2024, recensé 27 documents correspondant aux procès-verbaux des réunions du groupe de coopération SRI, de sa première à sa 27e réunion.

---

1 Enregistrée sous la référence EASE 2023/4388.
2 JO L 145 du 31.5.2001, p. 43.
3 Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, JO L 194 du 19.7.2016, p. 1, Directive - 2016/1148 - FR - EUR-Lex (europa.eu).
4 Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2), JO L 333 du 27.12.2022, p. 80, Directive - 2022/2555 - FR - EUR-Lex (europa.eu).
5 https://digital-strategy.ec.europa.eu/en/library/nis-cooperation-group-meetings-agendas.
6 C(2024) 5942.

La Commission a accordé un accès partiel à ces 27 documents, avec des occultations fondées sur les exceptions prévues à l'article 4, paragraphe 1, point a) (protection de l'intérêt public en ce qui concerne la sécurité publique) et à l'article 4, paragraphe 1, point b) (protection de la vie privée et de l'intégrité de l'individu) du règlement (CE) nº 1049/2001.

En outre, la Commission a fourni les adresses des pages web où ses lignes directrices sur l'application de l'article 3, paragraphe 4, de la directive SRI 2 et ses lignes directrices sur l'application de l'article 4, paragraphes 1 et 2, de la directive SRI 2 étaient accessibles au public[7].

En ce qui concerne le procès-verbal de la 28e réunion du groupe de coopération SRI, ladite réunion a eu lieu les 27 et 28 septembre 2023. La demande initiale ayant été présentée le 26 juillet 2023, la Commission a informé le demandeur que le procès-verbal de la 28e réunion sortait du périmètre de la demande.

II. PLAINTE AUPRÈS DE LA MÉDIATRICE EUROPÉENNE

Le demandeur a déposé une plainte auprès de la Médiatrice pour défaut de réponse dans le délai légal et refus de divulgation des documents. En outre, il a fait valoir que la Commission n'avait pas recensé tous les documents correspondant à sa demande. En particulier, il a affirmé que la Commission aurait dû recenser les procès-verbaux des 16e, 17e, 27e et 28e réunions (et y donner accès), étant donné que ces réunions figuraient sur le site internet de la Commission énumérant les ordres du jour de toutes les réunions du groupe de coopération SRI.

III. ENQUÊTE ET RECOMMANDATION DE LA MÉDIATRICE EUROPÉENNE

La Médiatrice a ouvert une enquête sur cette plainte et, compte tenu du retard pris pour adopter une décision, elle a demandé à la Commission d'examiner les documents en cause.

Dans sa proposition, la Médiatrice a estimé que la Commission aurait dû accorder un accès partiel étendu aux documents.

La Médiatrice a considéré que la Commission, bien que jouissant d'une large marge d'appréciation pour décider de ce que la protection de la sécurité publique exige s'agissant de la divulgation de documents, était néanmoins tenue de démontrer l'existence d'un risque pour la sécurité publique raisonnablement prévisible et non purement hypothétique.

À la suite de l'examen effectué par son équipe d'enquête, la Médiatrice a estimé que les documents, «dans une très large mesure, ne semblent pas contenir d'éléments sensibles: les procès-verbaux sont rédigés en des termes plutôt généraux et ne fournissent aucun détail sensible sur les travaux opérationnels concrets des autorités compétentes en matière de SRI. Il

[7] https://digital-strategy.ec.europa.eu/en/library/commission-guidelines-application-article-34-directive-eu-20222555-nis-2-directive et https://digital-strategy.ec.europa.eu/en/library/commission-guidelines-application-article-4-1-and-2-directive-eu-20222555-nis-2-directive.

semble que les contenus ou exposés sensibles aient été partagés avec les membres du groupe de coopération SRI au moyen d'une plateforme sécurisée […]».

Toutefois, la Médiatrice a relevé que, dans plusieurs documents[8], certains points de discussion pouvaient révéler des détails opérationnels. Ceux-ci concernent, entre autres, «la guerre en Ukraine, la manière dont les États membres appliquent les sanctions, les activités de certains pays tiers, les scénarios relatifs à des attaques à grande échelle visant le secteur de l'énergie ou les exposés des États membres au sujet de cyberattaques majeures récentes».

En outre, la Médiatrice a estimé qu'«une grande partie des discussions porte sur la communication, par les États membres, d'informations actualisées concernant leur transposition de la première directive SRI, sur les points de vue relatifs à la révision de la directive, ou encore sur l'état d'avancement de la transposition de la directive SRI 2». Selon la Médiatrice, compte tenu du temps écoulé, «il est difficile de voir comment ces aspects peuvent être considérés comme sensibles et, partant, relever de l'exception relative à la sécurité publique».

En ce qui concerne les données à caractère personnel figurant dans les documents, la Médiatrice a fait observer qu'elles pouvaient facilement être occultées.

En outre, la Médiatrice a estimé que la Commission aurait effectivement dû recenser trois des documents supplémentaires indiqués par le plaignant (les procès-verbaux des 16e, 17e et 27e réunions) et y accorder un accès partiel étendu, pour les mêmes raisons que celles exposées ci-dessus. En ce qui concerne le procès-verbal de la 28e réunion, la Médiatrice a considéré que ce document avait été finalisé après l'introduction de la demande du plaignant et qu'il n'entrait donc pas dans son périmètre.

La Médiatrice a fait observer que la décision d'exécution (UE) 2017/179 de la Commission[9] indiquait expressément que les délibérations du groupe ne sont pas ouvertes au public. Toutefois, à la lumière de l'article 10, paragraphe 1[10], et de l'article 10, paragraphe 3[11], de ladite décision d'exécution, la Médiatrice a estimé que la Commission devait fonder son appréciation de la demande d'accès du public sur les dispositions du règlement (CE) nº 1049/2001.

Compte tenu de ce qui précède, la Médiatrice a proposé que la Commission revoie sa position sur la demande du plaignant, en vue d'accorder l'accès le plus étendu possible aux

---

8 Documents numérotés 9, 13, 17, 20 et 21.

9 Décision d'exécution (UE) 2017/179 de la Commission du 1er février 2017 fixant les modalités de procédure nécessaires au fonctionnement du groupe de coopération conformément à l'article 11, paragraphe 5, de la directive (UE) 2016/1148 du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, C/2017/0438, JO L 28 du 2.2.2017, p. 73.

10 Les demandes adressées au groupe en vue d'accéder aux documents concernant ses activités sont traitées par la Commission conformément au règlement (CE) nº 1049/2001.

11 Les documents transmis aux membres du groupe, aux représentants de tierces parties et aux experts ne sont pas divulgués au public, sauf si l'accès à ces documents est accordé conformément au paragraphe 1 ou s'ils sont rendus publics par la Commission.

documents, y compris aux trois documents supplémentaires qui n'avaient pas été recensés au stade initial.

IV. RÉPONSE DE LA COMMISSION EUROPÉENNE À LA RECOMMANDATION DE LA MÉDIATRICE EUROPÉENNE

Dans sa décision confirmative, la Commission a recensé 27 procès-verbaux de réunions du groupe de coopération SRI, conformément à l'avis de la Médiatrice à ce sujet.

La Commission a accordé un accès partiel aux 27 documents, considérant que certaines parties de ceux-ci étaient couvertes par l'exception relative à la sécurité publique prévue à l'article 4, paragraphe 1, point a), du règlement (CE) nº 1049/2001. En outre, les données à caractère personnel ont été protégées au titre de l'exception prévue à l'article 4, paragraphe 1, point b) (protection de la vie privée et de l'intégrité de l'individu), dudit règlement.

La Médiatrice a recommandé à la Commission d'accorder l'accès le plus étendu possible aux documents. La Commission estime que, par sa décision confirmative C(2024) 5942, elle a satisfait à l'exigence relative à l'accès le plus étendu possible aux documents concernés, compte tenu des risques que leur divulgation entraînerait pour la sécurité publique, comme expliqué en détail dans la décision. En ce qui concerne la motivation, la Commission a expliqué, à suffisance de droit, en quoi l'accès aux parties occultées des documents pourrait concrètement et effectivement porter atteinte à l'intérêt protégé par l'exception prévue à l'article 4, paragraphe 1, point a), du règlement (CE) nº 1049/2001. La Commission a également démontré que le risque d'atteinte à cet intérêt était raisonnablement prévisible et non purement hypothétique.

La Commission n'est pas d'accord avec certaines des affirmations formulées par la Médiatrice dans sa proposition.

La Commission tient tout d'abord à souligner que les documents demandés par le demandeur sont les procès-verbaux des réunions du groupe de coopération pour la sécurité des réseaux et des systèmes d'information (ci-après le «groupe de coopération SRI»).

Comme expliqué dans la décision, le groupe de coopération SRI a été créé par la directive SRI[12] afin de garantir la coopération et l'échange d'informations entre les États membres. Dans le contexte d'une cybermenace grandissante et de la dépendance croissante de la société à l'égard des réseaux et des systèmes d'information, l'objectif de la directive est d'améliorer la résilience et les capacités de réponse aux incidents des entités publiques et privées, des autorités compétentes et de l'UE dans son ensemble dans le domaine de la cybersécurité et de la protection des infrastructures critiques. La directive vise à renforcer la coopération européenne tant au niveau politique (par l'intermédiaire du groupe de coopération SRI) qu'au niveau technique [dans le cadre des centres de réponse aux incidents de sécurité informatique

[12] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2), JO L 333 du 27.12.2022. Cette directive a succédé à la directive SRI 1.

(CSIRT)[13]] et à améliorer la gestion des crises [par la création du réseau européen pour la préparation et la gestion des crises cyber (EU-CyCLONe)]. Outre ce cadre juridique, la Commission européenne et le haut représentant de l'Union pour les affaires étrangères et la politique de sécurité ont présenté fin 2020 une nouvelle stratégie de cybersécurité de l'UE[14]. Cette stratégie met l'accent sur le renforcement des capacités collectives de réaction aux cyberattaques majeures et sur la collaboration avec des partenaires du monde entier pour garantir la sécurité et la stabilité internationales dans le cyberespace.

L'article 14 de la directive (UE) 2022/2555 (SRI 2) précise les tâches du groupe de coopération SRI. Il prévoit aussi que «[l]es États membres font en sorte que leurs représentants au sein du groupe de coopération puissent coopérer de manière effective, efficace et sécurisée». Le fonctionnement du groupe de coopération SRI est régi par la décision d'exécution de la Commission du 1er février 2017.

Le groupe de coopération SRI est composé de représentants des États membres, de la Commission et de l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA). Le secrétariat du groupe est assuré par la Commission européenne[15]. La Commission publie les ordres du jour de toutes les réunions du groupe de coopération SRI[16]. En règle générale, le groupe se réunit quatre fois par an.

Les sujets abordés lors de ces réunions et consignés dans les documents correspondants concernent les tâches assignées au groupe par la directive SRI 2.

Selon la Médiatrice, la plupart des documents ne semblent contenir aucun élément sensible.

Comme expliqué dans la décision, certaines parties des documents contiennent les avis et les points de vue des États membres sur les éléments livrables (concernant la cybersécurité de la 5G, par exemple), des informations au sujet de l'état d'avancement des activités relevant de tous les axes de travail, ainsi que des renseignements relatifs à d'autres mesures et discussions actuelles et futures aux niveaux national et transfrontière. Elles contiennent également des informations sur les incidents et les autres actions en cours dans les États membres. Elles rendent compte de discussions concernant la cybersécurité en lien avec des questions spécifiques telles que les élections européennes de 2019, la mise en œuvre des recommandations de la Commission, l'état d'avancement et la mise à jour des différentes mesures, y compris la mise en œuvre des recommandations du groupe, les travaux relatifs au réseau des CSIRT et la stratégie de cybersécurité de l'UE.

La Commission estime que la divulgation publique de ces parties des documents porterait atteinte à la protection de la sécurité publique, car elle fournirait au grand public, y compris aux personnes ou groupes malintentionnés, des informations utiles sur la lutte contre les cyberattaques. De l'avis de la Commission, cela rendrait les États membres et l'Europe totalement vulnérables face aux incidents et aux menaces en matière de sécurité.

---

13 Centres de réponse aux incidents de sécurité informatique: https://csirtsnetwork.eu.
14 https://digital-strategy.ec.europa.eu/fr/policies/cybersecurity-policies.
15 Article 14, paragraphe 3, de la directive SRI 2.
16 https://digital-strategy.ec.europa.eu/en/library/nis-cooperation-group-meetings-agendas.

La Commission partage l'avis de la Médiatrice selon lequel certaines informations contenues dans les documents pourraient, à première vue, sembler inoffensives, notamment du point de vue des utilisateurs ordinaires. Toutefois, elle tient à souligner que ces informations, placées dans un certain contexte, pourraient fournir des renseignements précieux au monde extérieur, y compris à d'éventuels cybercriminels. La Commission a procédé à une appréciation individuelle de chaque document et a recensé toutes les informations dont la divulgation présenterait un risque pour la sécurité publique. Ces informations ont été occultées. Il s'agit notamment des caractéristiques relatives à la plateforme utilisée pour l'échange d'informations par les membres du groupe de coopération SRI, mentionnée par la Médiatrice dans sa proposition de solution, et que la Commission souhaiterait demander à la Médiatrice de garder confidentielles. Même s'il est clair que des informations pertinentes supplémentaires ont été échangées entre les participants concernant les sujets abordés lors des réunions, les modalités concrètes du partage d'informations sensibles entre les participants devraient rester protégées. Compte tenu des efforts déployés par l'UE pour prévenir la cybercriminalité, décrits ci-dessus, la Commission considère que la prévention des attaques dans le domaine même de la lutte contre les cyberattaques est une priorité.

En ce qui concerne l'application du règlement (CE) nº 1049/2001 en l'espèce, l'article 10 de la décision d'exécution (UE) 2017/179 de la Commission[17] fixant les modalités de procédure nécessaires au fonctionnement du groupe de coopération SRI dispose que les demandes d'accès à des documents concernant les activités du groupe de coopération SRI seront traitées conformément audit règlement. Toutefois, la même base juridique définit le cadre particulier et spécifique dans lequel le groupe de coopération SRI mène ses activités. Elle précise d'emblée que les délibérations du groupe ne seront pas ouvertes au public. La Commission estime que, lors de l'appréciation de la demande, elle ne peut pas faire abstraction du caractère sensible des activités dont il est rendu compte dans les documents ni des finalités de la coopération dans ce domaine.

Il convient de rappeler que l'objectif du groupe de coopération SRI, tel que précisé dans la directive SRI 2 et la décision d'exécution, est de soutenir et de faciliter la coopération stratégique et l'échange d'informations, ainsi que de renforcer la confiance entre les États membres. En l'absence de confiance entre ses membres, le groupe de coopération ne pourrait pas accomplir sa mission générale. La coopération stratégique entre les États membres et le partage des informations, de l'expérience et des bonnes pratiques relatives à la sécurité des réseaux et des systèmes d'information sont essentiels pour répondre efficacement aux problèmes posés par les incidents et les risques liés à la sécurité de ces systèmes dans l'ensemble de l'Union.

Le groupe de coopération SRI travaille en étroite collaboration avec les États membres pour renforcer la sécurité dans tous les secteurs et atteindre un niveau élevé de protection contre les

[17] Décision d'exécution (UE) 2017/179 de la Commission du 1er février 2017 fixant les modalités de procédure nécessaires au fonctionnement du groupe de coopération conformément à l'article 11, paragraphe 5, de la directive (UE) 2016/1148 du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, C/2017/0438, JO L 28 du 2.2.2017, p. 73.

incidents de cybersécurité susceptibles d'avoir des répercussions significatives sur l'économie et la société européennes. En raison de la dimension européenne de cet objectif, le groupe travaille en étroite coopération et dans la confiance mutuelle avec ses membres et les autorités nationales afin de garantir la coopération transfrontière. La sécurité publique de l'Union est, par sa nature même, intrinsèquement liée au maintien d'un niveau élevé commun de cybersécurité dans l'ensemble de l'Union.

La Commission estime que la divulgation des discussions reproduites dans les documents demandés compromettrait la confiance et la coopération dans le domaine de la cybersécurité; or la coopération des autorités des États membres est indispensable à la cybersécurité. Le fait que certains documents datent de 2017 ne modifie pas le niveau de risque qu'entraînerait leur divulgation, étant donné qu'ils sont étroitement liés aux discussions et aux mesures actuelles. Le risque pour l'intégrité de l'architecture européenne de cybersécurité est toujours réel et non hypothétique. En outre, la Commission estime qu'il ne faut pas sous-estimer l'effet dissuasif que pourrait avoir la divulgation intégrale des procès-verbaux, qui saperait la bonne coopération entre les États membres et les autres participants aux réunions, ainsi que la confiance établie au sein du groupe de coopération SRI.

Comme expliqué dans la décision, la divulgation des parties occultées des documents donnerait une vue d'ensemble des risques, des vulnérabilités et des mesures d'atténuation des risques dans l'Union et pourrait mettre en évidence d'éventuelles lacunes dans les mesures d'atténuation existantes. La divulgation intégrale des documents demandés nuirait également à la capacité des opérateurs de réseau et des autorités publiques des États membres à protéger efficacement leurs réseaux contre les menaces en matière de cybersécurité. Cela pourrait avoir des conséquences négatives sur la sécurité des données ainsi que des systèmes informatiques actuels et futurs et entraîner des risques potentiels pour la sécurité de la société dans son ensemble.

En outre, la Médiatrice a estimé que les informations actualisées fournies par les États membres concernant leur transposition de la première directive SRI ou leur position sur la révision et la transposition de la directive SRI 2 ne revêtaient aucun caractère sensible et n'étaient pas couvertes par l'exception relative à la sécurité publique. La Commission ne partage pas l'avis de la Médiatrice sur ce point.

Certaines parties occultées des documents concernent l'état d'avancement de la transposition des directives SRI et SRI 2 en droit national. Si la transposition de la directive SRI 2 est toujours en cours, celle de la directive SRI est terminée. Toutefois, les parties concernées ont trait aux différentes mesures prises par les États membres à cet égard, ou aux solutions qui n'ont pas été retenues. La divulgation de ces parties des documents aurait une incidence négative sur la sécurité publique s'agissant des mesures prises au niveau national. Le temps n'a pas d'effet sur le niveau de risque, étant donné que les mesures décrites restent les plus pertinentes pour lutter contre la cybercriminalité.

Par conséquent, ces informations doivent également être protégées au titre de l'exception relative à la protection de l'intérêt public en ce qui concerne la sécurité publique.

V. CONCLUSIONS

Pour les raisons exposées ci-dessus, la Commission considère que l'accès le plus large possible a été accordé aux documents demandés, y compris aux trois documents supplémentaires qui n'avaient pas été recensés au stade initial.

Par la Commission
Věra JOUROVA
Vice-présidente