Observations formelles du CEPD sur le projet de règlement délégué de la Commission complétant le règlement (UE) 2019/943 du Parlement européen et du Conseil établissant un code de réseau sur les règles sectorielles concernant les aspects liés à la cybersécurité des flux transfrontaliers d'électricité

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le traité sur le fonctionnement de l'Union européenne,

vu le règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE (le «RPDUE»)[1], et notamment son article 42, paragraphe 1,

A ADOPTÉ LES OBSERVATIONS FORMELLES SUIVANTES:

1. Introduction et contexte

1. Le 23 octobre 2023, la Commission européenne a consulté le CEPD sur le projet de règlement délégué de la Commission complétant le règlement (UE) 2019/943 du Parlement européen et du Conseil établissant un code de réseau sur les règles sectorielles concernant les aspects liés à la cybersécurité des flux transfrontaliers d'électricité (le «projet de règlement délégué»).
2. L'objectif du projet de règlement délégué est d'adopter un processus récurrent d'évaluation des risques de cybersécurité dans le secteur de l'électricité[2]. Le modèle de gouvernance prévu par le projet de règlement délégué poursuit l'objectif d'harmoniser et de garantir une base de référence commune tout en respectant autant que possible les pratiques et les investissements existants[3]. Parmi les autres éléments du projet de règlement délégué figurent, entre autres, la promotion d'un cadre commun en matière de cybersécurité de l'électricité favorisant un niveau minimal commun de cybersécurité de l'électricité dans l'ensemble de l'Union, et l'adoption de règles pour la collecte et le partage d'informations relatives aux flux transfrontaliers

[1] JO L 295 du 21.11.2018, p. 39.
[2] Exposé des motifs, p. 1.
[3] Exposé des motifs, p. 1.

EUROPEAN DATA PROTECTION SUPERVISOR
Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30 - B-1000 Brussels
E-mail: edps@edps.europa.eu
Website: edps.europa.eu
Tel.: 32 2-283 19 00 - Fax: 32 2-283 19 50

d'électricité, compatibles avec d'autres législations nationales et législations de l'Union[4].

3. Le projet de règlement délégué est adopté conformément à l'article 59, paragraphe 2, point e), du règlement (UE) nº 2019/943[5].

4. Les présentes observations formelles du CEPD sont formulées en réponse à une consultation de la Commission européenne, réalisée conformément à l'article 42, paragraphe 1, du RPDUE. Le CEPD se félicite de la référence faite à cette consultation au considérant 31 du projet de règlement délégué.

5. Les présentes observations formelles n'empêchent pas le CEPD de formuler d'éventuelles observations supplémentaires à l'avenir, en particulier si de nouvelles questions sont soulevées ou si de nouvelles informations deviennent disponibles, par exemple à la suite de l'adoption d'autres actes d'exécution ou actes délégués connexes[6].

6. En outre, ces observations formelles sont fournies sans préjudice de toute intervention future susceptible d'être effectuée par le CEPD dans le cadre des pouvoirs qui lui sont conférés par l'article 58 du RPDUE et se limitent aux dispositions du projet de règlement délégué pertinentes du point de vue de la protection des données.

2. Observations

7. Le CEPD précise que le projet de règlement délégué fait référence à plusieurs mesures de cybersécurité susceptibles de nécessiter le traitement de données à caractère personnel. Selon les informations fournies par la Commission, le projet de règlement délégué ne vise toutefois pas à imposer des obligations spécifiques en matière de collecte, de traitement, de stockage ou d'échange de données à caractère personnel. Par exemple, l'article 32, paragraphe 2, point a), du projet de règlement délégué, prévoit que la vérification des antécédents de certains membres du personnel peut faire l'objet de recommandations dans le cadre de contrôles minimaux de cybersécurité dans la chaîne d'approvisionnement. L'objet précis et l'ampleur des vérifications des antécédents dépendraient toutefois des lois, des réglementations et de la déontologie applicables.

[4] Exposé des motifs, p. 2.
[5] Règlement (UE) 2019/943 du Parlement européen et du Conseil du 5 juin 2019 sur le marché intérieur de l'électricité (refonte), JO L 158 du 14.6.2019, p. 54.
[6] Dans le cas d'autres actes d'exécution ou actes délégués ayant une incidence sur la protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel, le CEPD tient à rappeler qu'il doit également être consulté sur ces actes. Il en va de même en cas de modifications futures qui introduiraient de nouvelles dispositions ou modifieraient des dispositions existantes qui concernent directement ou indirectement le traitement de données à caractère personnel.

8. L'article 37, paragraphe 1, point a) i), impose aux entités à forte incidence et à incidence critique de garantir l'enregistrement à des fins de sécurité dans le but de détecter des anomalies et de recueillir des informations sur les incidents liés à la cybersécurité. Le CEPD rappelle que certaines mesures liées à la cybersécurité, y compris l'enregistrement de toute interaction machine-utilisateur, peuvent nécessiter le traitement de données à caractère personnel. Cependant, le projet de règlement délégué, qui mentionne la collecte de données parmi les mesures obligatoires, ne précise pas les détails de cette obligation.

9. Le projet de règlement délégué fait également référence au partage d'informations dans un grand nombre de ses articles, notamment à l'article 37, paragraphe 1, à l'article 45, paragraphes 7 et 8, et à l'article 46, paragraphe 7. Bien que ces informations portent sur des menaces ou des incidents en matière de sécurité et ne contiennent pas nécessairement des données à caractère personnel, l'article 37, paragraphe 6, dispose que les adresses IP peuvent figurer parmi les informations à communiquer. En outre, l'article 37, paragraphe 6, du projet de règlement délégué, prévoit que la présence d'«informations telles que des adresses URL ou IP compromises, des hachages ou tout autre attribut utiles pour replacer l'attaque dans son contexte et corréler celle-ci» constitue l'une des conditions préalables au signalement.

10. Le considérant 30 du projet de règlement délégué confirme que tout traitement de données à caractère personnel dans le cadre dudit règlement doit être conforme au RGPD et au RPDUE. Bien que le projet de règlement ne soit pas destiné à réglementer le traitement des données à caractère personnel en tant que tel, il peut en effet nécessiter ledit traitement lorsqu'il est intégré de manière incidente dans le type d'informations requises au sens des articles 36 et 37.

11. Dans ce contexte, le CEPD recommande de préciser dans quels cas le projet de règlement délégué vise à fournir une base juridique au sens de l'article 6 du RGPD et de l'article 5 du RPDUE. Le cas échéant, l'entité qui adopte la mesure peut se fonder sur une autre base juridique, précisée notamment à l'article 6, paragraphe 1, point f), du RGPD. Il convient toutefois de préciser que, dans ces cas, le règlement délégué n'établit aucune obligation juridique ni aucune autre base juridique pour le traitement des données à caractère personnel.

12. Si le projet de règlement délégué vise à fournir une base juridique pour le traitement des données, il devrait définir clairement les finalités du traitement et les catégories de données à caractère personnel qui peuvent être traitées, ainsi que la période de conservation de ces données. Le projet devrait aussi attribuer clairement les rôles des différents acteurs concernés en tant que responsable du traitement, responsable conjoint du traitement ou sous-traitant;

13. Enfin, le CEPD salue les efforts déployés dans le cadre de ce projet de règlement délégué afin d'éviter d'éventuels conflits avec la législation en matière de protection

de données et d'exiger l'anonymisation, le cas échéant, par exemple à l'article 45, paragraphe 7, point b).

Fait à Bruxelles, le 17 novembre 2023

(signature électronique)
Wojciech Rafał WIEWIÓROWSKI