Observations formelles du CEPD sur la décision d'exécution de la Commission établissant un plan type de sécurité, un plan type de continuité des activités et un plan type de rétablissement après sinistre conformément à l'article 59, paragraphe 4, du règlement (UE) 2018/1240

1. Introduction et contexte

Le système européen d'information et d'autorisation concernant les voyages (ETIAS) a été créé par le règlement (UE) 2018/1240[1] et impose à tous les ressortissants de pays tiers exemptés de l'obligation de visa de demander en ligne une autorisation de voyage avant la date de leur départ vers l'espace Schengen.

En vertu de l'article 59, paragraphe 4, du règlement (UE) 2018/1240, la Commission européenne est habilitée à adopter, par voie d'actes d'exécution, un plan type de sécurité et un plan type de continuité des activités et de rétablissement après sinistre. Les plans types adoptés par la Commission servent de base, après au besoin avoir été adaptés, au conseil d'administration de l'eu-LISA, au conseil d'administration de l'Agence européenne de garde-frontières et de garde-côtes et aux États membres lorsqu'ils adoptent leurs propres plans de sécurité et plans de continuité des activités et de reprise après sinistre garantissant la sécurité du système d'information ETIAS.

Les présentes observations formelles du CEPD sont formulées en réponse à la consultation législative de la Commission européenne du 15 avril 2021, réalisée conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725[2]. À cet égard, le CEPD se félicite de la référence faite à cette consultation dans le considérant 9 du projet de décision d'exécution.

Le CEPD tient à souligner que les présentes observations formelles ne l'empêchent pas de formuler à l'avenir d'éventuelles observations supplémentaires, en particulier si de nouveaux problèmes sont identifiés ou si de nouvelles informations deviennent disponibles, par exemple à la suite de l'adoption d'autres actes d'exécution ou
actes délégués connexes, conformément au règlement (UE) 2018/1240. En outre, ces observations formelles sont sans préjudice de toute action future que le CEPD pourrait entreprendre dans l'exercice de ses pouvoirs en vertu de l'article 58 du règlement (UE) 2018/1725.

[1] Règlement (UE) 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS) et modifiant les règlements (UE) nº 1077/2011, (UE) nº 515/2014, (UE) 2016/399, (UE) 2016/1624 et (UE) 2017/2226 (JO L 236 du 19.9.2018, p. 1-71).

[2] 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, JO L 295 du 21.11.2018, p. 39 (règlement 2018/1725).

2. Observations

Le CEPD note le fait que le projet d'annexe à la décision d'exécution de la Commission contient un guide méthodologique sur la manière de rédiger un plan type de sécurité, un plan type de continuité des activités et un plan de rétablissement après sinistre. Toutefois, seul l'appendice 10 de l'annexe des projets de décision d'exécution de la Commission peut pleinement être considéré comme un «plan type».

Le CEPD rappelle que l'article 59, paragraphes 2 et 3, du règlement (UE) 2018/1240 régit les mesures de sécurité «sans préjudice de l'article 22 du règlement (CE) n° 45/2001», remplacé ultérieurement par l'article 33 du règlement (UE) 2018/1725, et également sans préjudice du règlement (UE) 2016/679[3]. Cela signifie que les exigences relatives à la mise en place de mesures de sécurité dans le projet de décision d'exécution de la Commission ne se limitent pas seulement aux éléments de l'article 59 du règlement (UE) 2018/1240 mais doivent également être conformes à toutes les exigences découlant du règlement (UE) 2018/1725 et du règlement (UE) 2016/679.

Le CEPD rappelle en outre que l'article 33, paragraphe 1, du règlement (UE) 2018/1725 ainsi que l'article 32, paragraphe 1, du règlement (UE) 2016/679 exigent qu'une analyse de risque obligatoire «pour les droits et libertés des personnes physiques» soit incluse dans l'analyse de risque par le responsable du traitement ou le sous-traitant. Le CEPD a fourni des orientations sur cette exigence obligatoire dans ses lignes directrices sur les mesures de sécurité pour le traitement des données à caractère personnel[4].

Alors que les mesures traditionnelles ou générales de gestion des risques liés à la sécurité des données visent à protéger les réseaux et les systèmes d'information de l'organisation (et les données qu'ils contiennent), les articles susmentionnés de la législation sur la protection des données visent à protéger les personnes et leurs droits en protégeant leurs données. Les actifs à protéger dans le cadre de ces deux activités sont différents, ce qui pourrait aboutir, dans certaines circonstances, à des conclusions différentes.

Le CEPD note que les droits et libertés des personnes physiques en tant qu'actif à protéger n'ont pas été suffisamment pris en compte par les plans types. Par exemple, les définitions de l'«évaluation de l'impact sur l'activité», de l'«analyse d'impact», de l'«analyse des risques», du «plan de sécurité» et d'autres termes ne font pas référence aux personnes physiques en tant que personnes concernées et à leurs droits. Dans le même ordre d'idées, la section «C6. Contrôles et processus de sécurité» ne fait pas référence aux risques concernant les droits et libertés des personnes physiques.

[3] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

[4] https://edps.europa.eu/data-protection/our-work/publications/guidelines/security-measures-personal-data-processing_fr.

Le CEPD recommande d'intégrer les considérations relatives à la vie privée et à la protection des données dans la gestion des risques liés à la sécurité des données afin de garantir une approche holistique et de permettre des synergies dans la gestion de la sécurité des données et de la protection des informations traitées sans multiplier inutilement les efforts, et invite la Commission à modifier le projet de décision d'exécution en conséquence.

Le CEPD note également le fait que le document fait à plusieurs reprises référence à la norme américaine NIST 800-54 rev.4, et non à sa dernière version rev.5, qui inclut les «risques liés à la protection de la vie privée». Par exemple, la norme la plus récente, NIST 800-53 rev.5, inclut dans l'évaluation des risques (page 240) «la probabilité et l'impact des effets négatifs sur les personnes découlant du traitement des informations à caractère personnel identifiables», alors que tel n'était pas le cas de dans la précédente version (rev.4) de la même norme (page 152). Plusieurs autres normes nationales, telles que la dernière version de la norme allemande «BSI Grundschutz», tiennent également compte des droits et libertés des personnes physiques dans leur méthodologie.

Le CEPD recommande donc que la Commission, lorsqu'elle fait référence à une norme américaine, se réfère à la dernière version (rev.5) de la norme NIST 800-53, qui correspond davantage aux dispositions de l'article 32, paragraphe 1, du règlement (UE) 2016/679 et de l'article 33, paragraphe 1, du règlement (UE) 2018/1725.

Bruxelles, le 7 juin 2021

Wojciech Rafał WIEWIÓROWSKI
(signature électronique)