EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

10 mai 2021

Avis 7/2021

sur la proposition de règlement sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014 et (UE) nº 909/2014

edps.europa.eu

Le Contrôleur européen de la protection des données (CEPD) est une autorité indépendante de l'Union européenne, qui est chargée, en vertu de l'article 52, paragraphe 2, du règlement (UE) 2018/1725, «[e]n ce qui concerne le traitement de données à caractère personnel, [...] de veiller à ce que les libertés et droits fondamentaux des personnes physiques, notamment le droit à la protection des données, soient respectés par les institutions et organes de l'Union» et, en vertu de l'article 52, paragraphe 3, «[...] de conseiller les institutions et organes de l'Union et les personnes concernées pour toutes les questions concernant le traitement des données à caractère personnel». En vertu de l'article 58, paragraphe 3, point c), du règlement (UE) 2018/1725, le CEPD dispose du pouvoir d'«émettre, de sa propre initiative ou sur demande, des avis à l'attention des institutions et organes de l'Union ainsi que du public, sur toute question relative à la protection des données à caractère personnel».

Wojciech Wiewiorówski a été nommé Contrôleur le 5 décembre 2019 pour un mandat de cinq ans.

Le présent avis n'exclut pas que le CEPD formule ultérieurement des observations ou des recommandations supplémentaires, en particulier si d'autres problèmes sont détectés ou si de nouvelles informations apparaissent. En outre, le présent avis est sans préjudice de toute action future que pourrait entreprendre le CEPD dans l'exercice des pouvoirs que lui confère l'article 58 du règlement (UE) 2018/1725.

Synthèse

Le 24 septembre 2020, la Commission européenne a adopté une proposition de règlement sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014 et (UE) nº 909/2014 (ci-après la «proposition»). La proposition établit un cadre global pour la résilience opérationnelle numérique des entités financières de l'UE, fondé sur cinq domaines clés, à savoir la gestion des risques informatiques (chapitre II), la gestion, la classification et la notification des incidents liés à l'informatique (chapitre III), les tests de résilience opérationnelle numérique (chapitre IV), la gestion des risques liés aux tiers et la réglementation des prestataires critiques de services informatiques (chapitre V), ainsi que le partage d'informations (chapitre VI).

Le CEPD se félicite des objectifs de la proposition et estime qu'il est essentiel, pour la stabilité des marchés financiers de l'Union européenne, que les établissements financiers disposent d'un cadre de gestion des risques informatiques solide, complet et bien documenté.

Le CEPD souligne qu'il importe de veiller à ce que tout traitement effectué dans le cadre des opérations des entités financières soit fondé sur l'une des bases juridiques prévues à l'article 6 du RGPD. En outre, le CEPD rappelle l'importance, pour les entités financières, d'intégrer dans leur cadre de résilience opérationnelle numérique un mécanisme de gouvernance solide en matière de protection des données, qui définisse clairement les rôles et les responsabilités du responsable du traitement et du sous-traitant, ainsi que les activités de traitement qui auront lieu.

En ce qui concerne les transferts internationaux à des tiers prestataires de services informatiques établis dans un pays tiers, le CEPD rappelle que tout transfert international de données à caractère personnel doit se conformer aux exigences du chapitre V du RGPD telles qu'interprétées dans la jurisprudence de la CJUE, notamment l'arrêt *Schrems II*.

En ce qui concerne les dispositifs de partage d'informations et de renseignements sur les cybermenaces entre les entités financières, le CEPD souligne que la protection des données à caractère personnel ne constitue pas un obstacle au partage de renseignements dans le secteur financier. Au contraire, les obligations en matière de protection des données devraient être perçues comme des exigences fondamentales qui doivent être remplies pour garantir la protection des droits des individus. Dans ce contexte, le CEPD encourage également l'adoption dans le secteur financier de codes de conduite conformément à l'article 40 du RGPD, en vue notamment de définir clairement les rôles des principales parties prenantes dans le traitement des données à caractère personnel et de garantir un traitement équitable et transparent.

En ce qui concerne la publication de sanctions administratives, le CEPD recommande d'inclure, parmi les critères à prendre en considération par l'autorité compétente, les risques pour la protection des données à caractère personnel des individus. En outre, le CEPD rappelle que le principe de limitation de la conservation des données exige que les données à caractère personnel soient conservées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées.

En ce qui concerne la notification des violations de données, le CEPD fait remarquer que le libellé du considérant 42 de la proposition est incompatible avec l'article 33 du RGPD. Le CEPD recommande donc de supprimer la référence aux autorités de protection des données du considérant 42 de la proposition, ainsi que de modifier légèrement l'article 17 de la proposition conformément aux recommandations du présent avis.

Table des matières

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 16,

vu la charte des droits fondamentaux de l'Union européenne, et notamment ses articles 7 et 8,

vu le 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)[1],

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[2], et notamment son article 42, paragraphe 1,

A ADOPTÉ LE PRÉSENT AVIS:

1 CONTEXTE

1. Le 24 septembre 2020, la Commission européenne a adopté une proposition de règlement sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014 et (UE) n° 909/2014 (ci-après la «**proposition**»). La proposition établit un cadre global pour la résilience opérationnelle numérique des entités financières de l'UE, fondé sur cinq domaines clés, à savoir la gestion des risques informatiques (chapitre II), la gestion, la classification et la notification des incidents liés à l'informatique (chapitre III), les tests de résilience opérationnelle numérique (chapitre IV), la gestion des risques liés aux tiers et la réglementation des prestataires critiques de services informatiques (chapitre V), ainsi que le partage d'informations (chapitre VI).

2. La présente proposition fait partie d'un paquet de mesures qui comprend une proposition de règlement pour créer des marchés de crypto-actifs[3] (le «**règlement MICA**»), une proposition sur un régime pilote pour les infrastructures de marché reposant sur la technologie des registres distribués[4], ainsi qu'une proposition visant à clarifier ou modifier certaines règles relatives aux services financiers de l'Union[5]. Le CEPD a été consulté sur la proposition sur le régime pilote pour les infrastructures de marché reposant sur la technologie des registres distribués et a rendu son avis le 23 avril 2021[6]. Il a également été consulté, le 29 avril 2021, sur le règlement MICA et rendra son avis conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725.

3. Le 15 mars 2021, la Commission européenne a demandé au Contrôleur européen de la protection des données (ci-après le «CEPD») d'émettre un avis sur la proposition, conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725. Ces observations se limitent aux dispositions pertinentes de la proposition en matière de protection des données.

2 OBSERVATIONS GÉNÉRALES

4. Le CEPD relève que la proposition vise notamment à consolider et à mettre à niveau les exigences en matière de risques informatiques, scindées jusqu'à présent dans différentes

législations[7], à établir des règles qui complètent le régime de notification des incidents liés à l'informatique dans la législation financière sectorielle, ainsi qu'à supprimer tout chevauchement et double emploi existant8. En outre, elle établit des règles visant à coordonner les tests effectués par les entités financières et les autorités compétentes, ce qui facilitera la reconnaissance mutuelle, dans tous les États membres, des tests avancés pour les entités financières d'importance significative[9]. Par ailleurs, la proposition définit certains principes clés pour encadrer la gestion, par les entités financières, du risque lié aux tiers prestataires de services informatiques, en les assortissant d'un ensemble de droits contractuels fondamentaux en vue de consacrer certaines garanties minimales[10]. Enfin, la proposition vise à mettre en place un cadre facilitant le partage d'informations et de renseignements sur les cybermenaces entre les entités financières.

5. **Le CEPD se félicite des objectifs de la proposition et considère qu'il est essentiel, pour assurer la stabilité des marchés financiers de l'Union européenne, que les entités financières mettent en œuvre un cadre de gestion des risques informatiques solide, complet et bien documenté**, afin de faire face à leurs propres risques informatiques et de gérer les risques liés aux tiers prestataires de services informatiques, notamment par la conclusion d'accords contractuels appropriés pour l'utilisation des services informatiques. Le CEPD reconnaît en outre l'importance d'établir des règles claires en ce qui concerne le processus de gestion des incidents liés à l'informatique ainsi que l'étendue et les limites du partage d'informations et de renseignements sur les cybermenaces entre les entités financières[11].

6. Le CEPD relève que le considérant 32 de la proposition prévoit que les mécanismes volontaires de partage d'informations devraient être employés en parfaite conformité avec les règles applicables du droit de la concurrence de l'Union «*ainsi que d'une manière qui garantisse le* ***plein respect des règles de l'Union en matière de protection des données****, principalement le règlement (UE) 2016/679 du Parlement européen et du Conseil, en particulier dans le cadre du traitement de données à caractère personnel qui est nécessaire* ***aux fins des intérêts légitimes*** *poursuivis par le responsable du traitement ou par un tiers, tel que visé à l'article 6, paragraphe 1, point f), dudit règlement*». À cet égard, il convient de rappeler qu'en vertu de l'article 6, paragraphe 1, point f), du RGPD, le traitement est licite lorsqu'il est «*nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant*». Dans ce contexte, le CEPD attire l'attention sur l'avis du Groupe de travail «Article 29» sur la notion d'intérêt légitime du responsable du traitement[12], qui précise que ce fondement juridique exige une mise en balance des intérêts légitimes du responsable du traitement, ou de tout tiers auquel les données sont communiquées, et des intérêts ou droits fondamentaux de la personne concernée. Le résultat d'une telle mise en balance permettra de déterminer si cette base juridique peut être invoquée comme fondement juridique du traitement. Parallèlement, le CEPD souligne que la formulation actuelle du considérant 32 de la proposition peut prêter à confusion dans la mesure où elle semble retenir l'article 6, paragraphe 1, point f), du RGPD comme seule base juridique possible. Or, le CEPD estime que la possibilité d'invoquer, dans certains cas, les bases juridiques visées à l'article 6, paragraphe 1, point c) ou e), ne devrait pas être exclue. Par conséquent, le CEPD propose de supprimer de la proposition la dernière partie de la phrase du considérant 32, qui fait spécifiquement référence à l'article 6, paragraphe 1, point f), du RGPD.

7. En outre, le CEPD rappelle l'importance, pour les entités financières, d'intégrer dans leur cadre de résilience opérationnelle numérique un **mécanisme de gouvernance solide en matière de protection des données**, qui définisse clairement les rôles et les responsabilités du

responsable du traitement et du sous-traitant, ainsi que les activités de traitement qui auront lieu. Ce n'est qu'ainsi que les entités financières pourront garantir les droits des personnes concernées conformément au RGPD et veiller à s'acquitter de leurs obligations en matière de sécurité des données à caractère personnel (à savoir la mise en œuvre de mesures techniques et organisationnelles appropriées en matière de sécurité, la notification en temps utile des violations de données à caractère personnel à l'autorité de contrôle et aux personnes concernées, la réalisation d'analyses d'impact relatives à la protection des données, le cas échéant, etc.).

3 OBSERVATIONS PARTICULIÈRES

3.1 En ce qui concerne les transferts internationaux à des tiers prestataires de services informatiques établis dans un pays tiers

8. Le CEPD se félicite que l'article 26, paragraphe 2, de la proposition concernant l'évaluation préliminaire du risque de concentration informatique et autres accords de sous-traitance exige que, lorsque des accords contractuels relatifs à l'utilisation de services informatiques sont conclus avec un tiers prestataire de services informatiques établi **dans un pays tiers**, les entités financières tiennent compte d'un certain nombre de facteurs, en particulier **le respect de la protection des données**. À cet égard, le CEPD rappelle que tout transfert international de données à caractère personnel doit en tout état de cause respecter les exigences du chapitre V du RGPD telles qu'interprétées dans la jurisprudence de la CJUE, notamment l'arrêt *Schrems II*[13].

9. Le CEPD rappelle que, conformément à l'article 45, paragraphe 1, du RGPD, un transfert de données à caractère personnel vers un pays tiers peut avoir lieu lorsque la Commission a constaté par voie de décision que le pays tiers assure un niveau de protection adéquat (la décision d'adéquation). En l'absence d'une décision d'adéquation, les entités financières qui cherchent à externaliser des services ou à utiliser une infrastructure informatique impliquant un transfert de données à caractère personnel doivent procéder à une analyse de la sécurité du transfert, et peuvent recourir à des **clauses contractuelles types**, qui sembleraient être l'outil de transfert le plus pertinent. À cet égard, le CEPD attire l'attention sur l'avis conjoint 2/2021 de l'EDPB et du CEPD sur la décision d'exécution de la Commission européenne relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers pour les questions visées à l'article 46, paragraphe 2, point c), du règlement (UE) 2016/679[14].

10. Le CEPD se félicite que la proposition mentionne spécifiquement la protection des données à caractère personnel comme l'un des domaines essentiels auxquels les accords contractuels relatifs à l'utilisation de services informatiques doivent faire référence. En particulier, l'article 27, paragraphe 2, point c), de la proposition dispose que «*les accords contractuels relatifs à l'utilisation de services informatiques comportent des dispositions sur l'accessibilité, la disponibilité, l'intégrité, la sécurité* ***et la protection des données à caractère personnel*** *et sur la garantie de l'accès, de la récupération et de la restitution [...]*».

3.2 En ce qui concerne les dispositifs d'échange d'informations

11. Le CEPD relève qu'en ce qui concerne le partage de renseignements sur les menaces informatiques entre les entités financières, la proposition affirme qu'«*en l'absence d'orientations au niveau de l'Union,* ***plusieurs facteurs semblent avoir entravé ce partage de renseignements****, notamment l'incertitude quant à la compatibilité avec les règles en matière de protection des données, de pratiques anticoncurrentielles et de responsabilité*». À cet égard, le

CEPD rappelle que **la protection des données à caractère personnel ne constitue pas un obstacle au partage de renseignements** dans le secteur financier. Au contraire, les obligations en matière de protection des données devraient être perçues comme une exigence fondamentale, qui devrait être respectée afin de garantir la protection des droits des individus au sein du cadre de résilience opérationnelle numérique des entités financières. En outre, le CEPD rappelle le rôle important des autorités nationales de protection des données dans la sensibilisation du public et la compréhension des risques, des règles, des garanties et des droits liés au traitement[15], ainsi que dans la sensibilisation des responsables du traitement et des sous-traitants aux obligations qui leur incombent en vertu du RGPD[16]. Le CEPD attire également l'attention sur les orientations fournies par le comité européen de la protection des données dans ses lignes directrices, recommandations et bonnes pratiques, dans le but d'encourager une application cohérente du RGPD[17].

12. Le CEPD se félicite que la proposition subordonne l'échange d'informations et de renseignements sur les cybermenaces entre les entités financières à l'exigence que ce partage «repose sur des dispositifs de partage des informations qui protègent la *nature potentiellement sensible des informations partagées et qui sont* ***régis par des règles de conduite dans le plein respect de la confidentialité des affaires, de la protection des données à caractère personnel*** *et des lignes directrices sur la politique de concurrence*»[18]. À cet égard, **le CEPD encourage également l'adoption de codes de conduite dans le secteur financier conformément à l'article 40 du RGPD**, en vue notamment de définir clairement les rôles des principales parties prenantes dans le traitement des données à caractère personnel et de garantir un traitement équitable et transparent.

3.3 En ce qui concerne la publication de sanctions administratives

13. Le CEPD note que l'article 48, paragraphe 3, de la proposition autorise les autorités compétentes à adopter, dans certains cas, **des mesures alternatives à la publication de l'identité et des données à caractère personnel** des personnes physiques et morales auxquelles elles imposent une sanction administrative, notamment reporter sa publication jusqu'à ce qu'il n'existe plus aucune raison de ne pas la publier, **la publier en préservant l'anonymat des intéressés,** conformément au droit national, ou s'abstenir de la publier, si les deux options précédentes sont jugées insuffisantes pour garantir l'absence totale de risque pour la stabilité des marchés financiers, ou si cette publication ne serait pas proportionnée, eu égard à la clémence de la sanction imposée[19]. Ces mesures alternatives peuvent être prises lorsque, après une évaluation au cas par cas, l'autorité compétente estime que la publication serait disproportionnée, compromettrait la stabilité des marchés financiers ou la poursuite d'une enquête pénale en cours, ou causerait, dans la mesure où ils peuvent être déterminés, des dommages disproportionnés à la personne concernée. **Le CEPD recommande d'inclure, parmi les critères à prendre en considération par l'autorité compétente, les risques pour la protection des données à caractère personnel des individus.**

14. Le CEPD relève que l'article 48, paragraphe 6, de la proposition dispose que les autorités compétentes veillent à ce que toute publication de sanction administrative «*demeure sur leur site web officiel pendant une période d'au moins* ***cinq ans*** *après sa publication.* ***Les données à caractère personnel*** *figurant dans une telle publication* ***ne sont maintenues*** *sur le site web officiel de l'autorité compétente* ***que pour la durée nécessaire au sens des règles applicables en matière de protection des données***». Le CEPD rappelle que le principe de limitation de la conservation des données exige que les données à caractère personnel soient conservées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées. Les entités financières devraient donc prendre des mesures pour faire en sorte que les informations relatives aux sanctions administratives soient supprimées

de leur site web après l'expiration du délai de cinq ans, ou avant, si elles ne sont plus nécessaires.

3.4 En ce qui concerne la notification des violations de données

15. Conformément au considérant 42 de la proposition, «*la notification directe permettrait aux autorités de surveillance financière d'avoir accès aux informations sur les incidents liés à l'informatique. Néanmoins,* ***les autorités de surveillance financière devraient transmettre ces informations aux autorités publiques non financières*** *(autorités compétentes en matière de sécurité des réseaux et des systèmes d'information, autorités nationales de protection des données et services répressifs pour les incidents de nature criminelle)*». En outre, l'article 17 de la proposition exige que les entités financières notifient à l'autorité compétente pertinente visée à l'article 41 les incidents majeurs liés à l'informatique, dans les délais prévus au paragraphe 3.

16. Il convient de souligner que le libellé du **considérant 42 de la proposition est incompatible avec l'article 33 du RGPD**, qui impose au responsable du traitement, en cas de violation de données, l'obligation directe d'en notifier la violation à l'autorité de contrôle compétente, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance. Le CEPD recommande donc de supprimer la référence aux autorités de protection des données du considérant 42 de la proposition, ainsi que d'inclure le libellé suivant à l'article 17 de la proposition: «*Lorsque l'incident majeur lié à l'informatique relève également d'une violation de données à caractère personnel, les entités financières en notifient la violation à l'autorité de protection des données compétente et à la (aux) personne(s) concernée(s), le cas échéant, conformément à l'article 33 du RGPD*».

17. Néanmoins, le CEPD convient que les différents types de notifications requis par les divers actes de l'UE peuvent comporter des informations très similaires. Dès lors, il estime qu'à plus long terme, l'idée d'un pôle central, mentionnée au considérant 43, est inévitable. Le CEPD est prêt à discuter de cette possibilité et à associer d'autres autorités de contrôle du RGPD à cette discussion, qui ne devrait pas être limitée à l'ESA, à la BCE et à l'ENISA.

18. En outre, le CEPD souligne que le terme «*fuite d'informations*», employé à l'article 8, paragraphe 3, point c), de la proposition, n'est pas défini. Afin d'éviter toute confusion, le CEPD recommande de remplacer ce terme par les termes «atteinte à la sécurité informatique» ou «violation de la confidentialité», qui sont déjà utilisés dans la proposition.

19. Le CEPD note que l'article 23, paragraphe 2, de la proposition exige que «*les tests de pénétration fondés sur la menace couvrent au minimum les fonctions et les services critiques d'une entité financière et sont effectués sur des systèmes de production en direct qui appuient ces fonctions*». Le CEPD estime que les tests, le développement de produits ou la recherche liée aux systèmes informatiques ne devraient pas être effectués sur des systèmes de production en direct contenant des données à caractère personnel des clients[20]. Par conséquent, le CEPD recommande de modifier la disposition susmentionnée comme suit: «*(...) ne sont effectués sur des systèmes de production en direct qui appuient ces fonctions que si les systèmes ne contiennent pas de données à caractère personnel*» (soulignement ajouté).

4 CONCLUSIONS

À la lumière de ce qui précède:

- Le CEPD rappelle l'importance de veiller à ce que **toute opération de traitement** effectuée dans le cadre des activités des entités financières **soit fondée sur l'une des bases juridiques visées à l'article 6 du RGPD**, en indiquant l'article 6, paragraphe 1, points c), e) et f), du RGPD comme une base juridique possible pour les entités financières.
- Le CEPD insiste sur l'importance, pour les entités financières, d'intégrer dans leur cadre de résilience opérationnelle numérique un **mécanisme de gouvernance solide en matière de protection des données**, qui définisse clairement les rôles et les responsabilités du responsable du traitement et du sous-traitant, ainsi que les activités de traitement qui auront lieu.
- Le CEPD rappelle que **tout transfert international de données à caractère personnel par des entités financières** à un tiers prestataire de services informatiques établi dans un pays tiers **doit respecter les exigences du chapitre V du RGPD** et, le cas échéant, faire l'objet de garanties appropriées conformément au cadre de protection des données et à la jurisprudence de la CJUE, en particulier l'arrêt Schrems II. Ces entités financières peuvent recourir aux clauses contractuelles types, qui sembleraient être l'outil de transfert le plus pertinent.
- Le CEPD souligne que la **protection des données à caractère personnel ne constitue pas un obstacle au partage de renseignements dans le secteur financier**. Au contraire, les obligations en matière de protection des données devraient être perçues comme une exigence fondamentale qui doit être remplie pour garantir la protection des droits des individus au sein du cadre de résilience opérationnelle numérique des entités financières.
- Le CEPD **encourage également l'adoption de codes de conduite dans le secteur financier** conformément à l'article 40 du RGPD, en vue notamment de définir clairement les rôles des principales parties prenantes dans le traitement des données à caractère personnel et de garantir un traitement équitable et transparent.
- En ce qui concerne la **publication de sanctions administratives**, le CEPD recommande d'inclure, parmi les critères à prendre en considération par l'autorité compétente, **les risques pour la protection des données à caractère personnel des individus**.
- Conformément au principe de limitation de la conservation, le CEPD recommande aux entités financières de prendre des mesures visant à faire en sorte que les **informations relatives aux sanctions administratives soient supprimées de leur site web après l'expiration du délai de cinq ans, ou avant**, si elles ne sont plus nécessaires.
- Le CEPD souligne que le **libellé du considérant 42 de la proposition est incompatible avec l'article 33 du RGPD**. Le CEPD recommande donc de supprimer la référence aux autorités de protection des données du considérant 42 de la proposition, ainsi que de modifier l'article 17 de la proposition afin d'y inclure une référence à l'obligation de notification des violations de données aux autorités compétentes en matière de protection des données.
- Le CEPD recommande de modifier l'article 23, paragraphe 2, de la proposition afin que les tests, le développement de produits ou la recherche liée aux systèmes informatiques ne puissent pas être effectués sur des systèmes de production en direct contenant des données à caractère personnel de clients.

Bruxelles, le 10 mai 2021

Wojciech Rafał WIEWIÓROWSKI

(signature électronique)

Notes

[1] *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).*

[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) n° 45/2001 et la décision n° 1247/2002/CE (JO L 295 du 21.11.2018).*

[3] *Proposition de règlement du Parlement européen et du Conseil sur les marchés de crypto-actifs, et modifiant la directive (UE) 2019/1937, COM/2020/593 final. Disponible à l'adresse suivante: EUR-Lex - 52020PC0593 - EN - EUR-Lex (europa.eu)*

[4] *Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL sur un régime pilote pour les infrastructures de marché reposant sur la technologie des registres distribués*

COM/2020/594 final, disponible à l'adresse suivante: EUR-Lex - 52020PC0594 - EN - EUR-Lex (europa.eu)

[5] *Proposition de directive du Parlement européen et du Conseil modifiant les directives 2006/43/CE, 2009/65/CE, 2009/138/UE, 2011/61/UE, 2013/36/UE, 2014/65/UE, (UE) 2015/2366 et (UE) 2016/2341, COM/2020/596 final. Disponible à l'adresse suivante: EUR-Lex - 52020PC0596 - EN - EUR-Lex (europa.eu)*

[6] *Avis 6/2021 sur la proposition sur un régime pilote pour les infrastructures de marché reposant sur la technologie des registres distribués, disponible à l'adresse suivante: 2021-0219_d0912_opinion_6_2021_en_0.pdf (europa.eu)*

[7] *Considérant 12*

[8] *Considérant 22*

[9] *Considérant 24*

[10] *Considérant 27*

[11] *À cet égard, voir plus généralement les lignes directrices du CEPD sur la protection des données à caractère personnel pour la gouvernance informatique et la gestion informatique des institutions européennes, qui peuvent également fournir des orientations, mutatis mutandis, dans le cas d'espèce.*

Les lignes directrices sont disponibles à l'adresse suivante:

it_governance_management_en.pdf (europa.eu)

[12] *Avis 06/2014 du Groupe de travail «Article 29» sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE, rendu le 9 avril 2014 et disponible à l'adresse suivante: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf*

[13] *Arrêt du 16 juillet 2020, C-311/18, Data Protection Commissioner contre Facebook Ireland Ltd et Maximillian Schrems*

[14] *https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_edps_jointopinion_202102_art46sccs_en.pdf*

[15] *Article 57, paragraphe 1, point b), du RGPD*

[16] *Article 57, paragraphe 1, point d), du RGPD*

[17] *Article 70, paragraphe 1, point e), du RGPD*

[18] *Article 40, paragraphe 1, point b), de la proposition*

[19] *Article 48, paragraphe 3, de la proposition*

[20] *Voir, à cet égard, les lignes directrices du CEPD sur la protection des données à caractère personnel pour la gouvernance informatique et la gestion informatique des institutions européennes, paragraphes 80, 81 et 82, disponibles à l'adresse suivante: https://edps.europa.eu/sites/edp/files/publication/it_governance_management_en.pdf, qui disposent que:*

80. Lors de la phase de test, il convient d'éviter l'échantillonnage de données à caractère personnel réelles, car celles-ci ne peuvent pas être utilisées à des fins pour lesquelles elles n'ont pas été collectées et les utiliser dans le cadre de tests pourrait les rendre accessibles à des personnes non autorisées.

81. Il est recommandé d'utiliser, si possible, des données artificiellement créées ou des données de test qui sont dérivées de données réelles, dont la structure a été préservée mais qui ne contient en fait aucune donnée à caractère personnel. Différentes techniques de ce genre ont été appliquées avec succès.

82. Lorsqu'une analyse complète et prudente montre que les données de test produites ne peuvent pas suffisamment garantir la validité des tests, une décision globale doit être prise et documentée, portant sur les données réelles, limitées au maximum, qui seront utilisées dans le test, ainsi que sur les garanties techniques et organisationnelles supplémentaires qui seront mises en place dans l'environnement

de test. Certaines catégories de données spéciales ne peuvent être utilisées dans des tests de données réelles qu'avec le consentement explicite des personnes concernées.