Observations formelles du CEPD sur le projet de proposition de règlement délégué de la Commission modifiant le règlement délégué (UE) 2018/389 de la Commission complétant la directive (UE) 2015/2366 du Parlement européen et du Conseil par des normes techniques de réglementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication

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 («RPDUE»)[1], et notamment son article 42, paragraphe 1,

A ADOPTÉ LES OBSERVATIONS FORMELLES SUIVANTES:

1. Introduction et contexte

1. La Commission européenne a rendu un projet de proposition de règlement délégué de la Commission modifiant le règlement délégué (UE) 2018/389 de la Commission complétant la directive (UE) 2015/2366 du Parlement européen et du Conseil par des normes techniques de réglementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication (le «projet de proposition»).

2. L'objectif du projet de proposition est de mettre à jour les normes techniques de réglementation (les «NTR») telles qu'adoptées dans le règlement délégué (UE) 2018/389 de la Commission[2] (le «règlement délégué») et applicables depuis le 14 septembre 2019.

3. Les NTR existantes ont été adoptées conformément à l'article 98, paragraphe 1 de la directive (UE) 2015/2366[3] (la «DSP2»), qui prévoit l'élaboration par l'Autorité

[1] JO L 295 du 21.11.2018, p. 39.

[2] Règlement délégué (UE) 2018/389 de la Commission du 27 novembre 2017 complétant la directive (UE) 2015/2366 du Parlement européen et du Conseil par des normes techniques de réglementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication (JO L 69 du 13.3.2018, p. 23).

[3] Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le

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

bancaire européenne («ABE») de NTR sur l'authentification forte du client («SCA») et des normes ouvertes communes et sécurisées de communication. L'article 98, paragraphe 5 de la DSP2 exige la révision et la mise à jour des NTR à intervalles réguliers.

4. Les présentes observations formelles du CEPD sont émises en réponse à une consultation de la Commission européenne du 2 mai 2022, conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725[4] (le «RPDUE»).

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[5].

6. En outre, ces observations formelles sont sans préjudice de toute mesure future qui pourrait être prise par le CEPD dans l'exercice des pouvoirs qui lui sont conférés par l'article 58 du RPDUE et se limitent aux dispositions du projet de proposition qui sont pertinentes du point de vue de la protection des données.

2. Observations

2.1. Nouvelles dérogations à l'utilisation de la SCA

7. Le CEPD note que l'article 1er du projet de proposition, qui remplacerait l'article 10 du règlement délégué par un nouvel article 10, introduit une modification de la

règlement (UE) nº 1093/2010, et abrogeant la directive 2007/64/CE (JO L 337 du 23.12.2015, p. 35). Voir également l'avis du Contrôleur européen de la protection des données sur une proposition de directive du Parlement européen et du Conseil concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2006/48/CE et 2009/110/CE et abrogeant la directive 2007/64/CE, ainsi que sur une proposition de règlement du Parlement européen et du Conseil relatif aux commissions d'interchange pour les opérations de paiement liées à une carte

[4] 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).

[5] 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.

dérogation à la SCA s'appliquant lorsqu'un client utilise un prestataire de services de paiement gestionnaire du compte («PSPGC») pour accéder directement à ses informations sur le compte de paiement et que cet accès est limité à un ou à deux des éléments suivants en ligne sans que des données de paiement sensibles soient divulguées:
(a) le solde d'un ou de plusieurs comptes de paiement désignés;
(b) les opérations de paiement exécutées durant les 90 derniers jours par l'intermédiaire d'un ou de plusieurs comptes de paiement désignés.
Dans ce cas, le délai pour le renouvellement obligatoire de la SCA est prolongé par l'article 10 modifié de 90 jours à 180 jours depuis la dernière fois que l'utilisateur de services de paiement a accédé en ligne à son compte de paiement et que la SCA a été appliquée[6].

8. L'article 1er, paragraphe 2, du projet de proposition introduirait un nouvel article 10 *bis* dans le règlement délégué, en ce qui concerne l'accès par un client à l'information sur le compte de paiement par l'intermédiaire d'un prestataire de services d'information sur les comptes («PSIC»). Dans ce cas, les prestataires de services de paiement n'appliquent pas la SCA lorsqu'un client utilise un PSIC pour accéder à ses informations sur le compte de paiement et que cet accès est limité à un ou à deux des éléments suivants en ligne sans que des données de paiement sensibles soient divulguées:
(a) le solde d'un ou de plusieurs comptes de paiement désignés;
(b) les opérations de paiement exécutées durant les 90 derniers jours par l'intermédiaire d'un ou de plusieurs comptes de paiement désignés.

9. Dans ce cas également (accès par l'intermédiaire d'un PSIC), comme prévu en cas d'accès direct avec le PSPGC, le délai pour le renouvellement obligatoire de la SCA est porté de 90 jours à 180 jours depuis la dernière fois que l'utilisateur de services de paiement a accédé en ligne à son compte de paiement et que la SCA a été appliquée. Le CEPD note également qu'en cas d'accès par l'intermédiaire d'un PSIC, les prestataires de services de paiement sont autorisés à appliquer une SCA lorsqu'un utilisateur de services de paiement accède à son compte de paiement en ligne et que le prestataire de services de paiement a des raisons objectivement motivées et documentées liées à un accès non autorisé ou frauduleux au compte de paiement[7].
En outre, les PSPGC qui offrent l'interface d'accès[8] sont autorisés à appliquer la SCA aux fins du mécanisme d'urgence au cas où l'interface d'accès ne fonctionnerait pas

[6] Voir article 10, paragraphe 2, point b).
[7] Voir article 10 *bis*, paragraphe 3.
[8] L'interface visé à l'article 31 du règlement délégué.

conformément à l'article 32 du règlement délégué, où elle serait indisponible de façon imprévue et où le système tomberait en panne[9].

10. Le CEPD rappelle que les «lignes directrices relatives à l'interaction entre la deuxième directive sur les services de paiement et le RGPD»[10] soulignent que les prestataires de services devraient être tenus d'appliquer des normes élevées, y compris des mécanismes d'authentification forte du client et des normes de sécurité élevées pour l'équipement technique.

11. Le CEPD note que le projet de proposition est fondé sur une vaste consultation publique où plusieurs ensembles de parties prenantes ont exprimé une opinion favorable quant aux modifications introduites, comme indiqué dans l'analyse d'impact réalisée par l'ABE[11].

12. Le CEPD approuve l'analyse menée par l'ABE, à savoir que les modifications introduites par le projet de proposition instaurent un bon équilibre entre l'expérience de l'utilisateur et le haut niveau de sécurité requis pour les services de paiement[12]. Par conséquent, le CEPD n'a pas d'autres recommandations à formuler à cet égard.

[9] Voir article 10 *bis*, paragraphe 4.

[10] Lignes directrices 6/2020 du CEPD relatives à l'interaction entre la deuxième directive sur les services de paiement et le RGPD, version 2.0, adoptées le 15 décembre 2020, paragraphe 71, page 23.

[11] Rapport final de l'ABE, projet de normes techniques de réglementation modifiant le règlement délégué (UE) 2018/389 de la Commission complétant la directive (UE) 2015/2366 du Parlement européen et du Conseil par des normes techniques de réglementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication, EBA/RTS/2022/03, 5 avril 2022 (le «rapport final de l'ABE»).

[12] Rapport final de l'ABE, paragraphe 17, page 9. En particulier, sur la dérogation à la SCA pour le PSIC, voir paragraphe 20, page 9; sur la modification de la fréquence de renouvellement de la SCA, voir paragraphe 27, page 11.

2.2. Absence de la référence à cette consultation dans un considérant du projet de proposition

13. À cet égard, le CEPD constate l'absence de la référence à cette consultation dans un considérant du projet de proposition. Par conséquent, le CEPD recommande d'insérer cette référence dans un considérant du projet de proposition.

Bruxelles, le 7 juin 2022

(signature électronique)
Wojciech Rafał Wiewiórowski