Directive sur les services de paiement («DSP2»): Normes techniques de réglementation permettant aux consommateurs de bénéficier de paiements électroniques plus sûrs et innovants

Bruxelles, le 27 novembre 2017

1. Justification, objectifs et processus

Quels sont les objectifs de la DSP2?

La directive révisée sur les services de paiement (DSP2), qui entre en application le 13 janvier 2018, favorisera l'innovation, la concurrence et l'efficience. Elle permettra d'élargir et d'améliorer le choix des consommateurs sur le marché des paiements de détail dans l'UE. Dans le même temps, elle instaurera des normes de sécurité plus strictes pour les paiements en ligne, ce qui renforcera la confiance des consommateurs dans les achats en ligne. Le champ d'application de la DSP2 s'étend aux services de paiement innovants et aux nouveaux fournisseurs sur le marché, tels que les sociétés de technologie financière (les «FinTech»). Ces acteurs sont également appelés prestataires de services de paiement tiers (PSP tiers). Les PSP tiers comprennent:

- les prestataires de services d'initiation de paiement (PSIP), qui offrent d'initier les paiements pour le compte de clients, donnant ainsi l'assurance aux détaillants que l'argent est en route.
- les agrégateurs et prestataires de services d'information sur les comptes (PSIC), qui fournissent à leurs clients une vue d'ensemble des comptes et soldes disponibles.

Quels sont les objectifs des normes techniques de réglementation?

Les acteurs du marché ont besoin d'exigences précises pour pouvoir se conformer aux nouvelles obligations de la DSP2. À cette fin, la DSP2 habilite la Commission à adopter des normes techniques de réglementation sur la base d'un projet présenté par l'Autorité bancaire européenne (ABE).

Les mesures de sécurité énoncées dans les normes techniques de réglementation découlent de deux objectifs clés de la DSP2: assurer la protection des consommateurs, et renforcer la concurrence et garantir des conditions de concurrence équitables dans un marché en mutation rapide.

La protection des consommateurs est assurée par une amélioration de la sécurité des paiements électroniques. C'est la raison pour laquelle les normes techniques de réglementation instaurent des exigences de sécurité que les prestataires de services de paiement doivent respecter lorsqu'ils traitent des opérations de paiement ou fournissent des services connexes. Les prestataires de services de paiement incluent les banques et les autres établissements de paiement. Ces normes définissent les exigences à remplir pour permettre une «authentification forte» des clients et précisent les cas dans lesquels les prestataires de services de paiement peuvent être dispensés de cette authentification.

Par ailleurs, un objectif clé est de stimuler la concurrence ainsi que l'innovation sur le marché des paiements de détail. Dans ce contexte, les normes techniques de réglementation incluent deux nouveaux types de services de paiement, à savoir les services d'initiation de paiement et les services d'information sur les comptes.

La Commission a-t-elle modifié les normes techniques de réglementation soumises par l'ABE?

La Commission a apporté un nombre limité de modifications de fond au projet de normes soumis par l'ABE, dans le souci de mieux refléter le mandat de la DSP2 et d'apporter plus de clarté et de sécurité pour toutes les parties intéressées.

Quand les nouvelles règles seront-elles applicables?

La DSP2 sera applicable à partir du 13 janvier 2018, sauf en ce qui concerne les mesures de sécurité visées dans ses articles 65, 66, 67 et 97 et décrites dans les normes techniques de réglementation. Ces mesures deviendront applicables 18 mois après la date d'entrée en vigueur des normes en question.

À quel type de comptes ces normes s'appliqueront-elles?

Les normes techniques de réglementation ne couvrent que les comptes de paiement qui entrent dans

le champ d'application de la DSP2, c'est-à-dire les comptes détenus par un ou plusieurs utilisateurs de services de paiement, qui peuvent servir à l'exécution d'opérations de paiement. Bien que cette définition n'ait pas changé avec l'adoption de la DSP2, la liste des services de paiement concernés a évolué. Elle inclut les services d'initiation de paiement et les services d'information sur les comptes.

2. Authentification forte du client

Comment les nouvelles normes techniques de réglementation renforceront-elles la sécurité des paiements électroniques?

Grâce à la DSP2, les consommateurs seront mieux protégés lorsqu'ils effectuent des paiements ou des transactions électroniques (dans le cadre de l'utilisation de leurs services de banque en ligne ou lors d'achats en ligne, par exemple). Les normes techniques de réglementation font de l'authentification forte la condition de base pour que le client puisse accéder à son compte de paiement ou effectuer des paiements en ligne.

Cela implique que, pour prouver son identité, l'utilisateur devra répondre au moins à deux des trois conditions suivantes:

- connaître un certain mot de passe ou code PIN;
- être en possession d'une certaine carte ou d'un certain téléphone mobile; et
- présenter certaines caractéristiques biométriques (empreintes digitales ou scan de l'iris, par exemple).

L'authentification forte du client est déjà communément employée dans l'ensemble de l'UE. Par exemple, lorsqu'un client paie avec sa carte bancaire dans un magasin physique, il doit valider l'opération en saisissant son code PIN sur un lecteur de carte. Ce n'est en revanche pas le cas pour les opérations de paiement électronique à distance, qu'il s'agisse de paiements par carte ou de virements depuis une banque en ligne. Pour ces opérations, l'authentification forte du client n'est appliquée que dans certains pays de l'UE (dont la Belgique, les Pays-Bas et la Suède). Dans d'autres, certains prestataires de services de paiement l'appliquent sur une base volontaire.

Les normes techniques de réglementation rendent l'authentification forte obligatoire pour l'accès du client à son compte de paiement et pour ses opérations de paiement en ligne. Les banques et les autres prestataires de services de paiement devront mettre en place les infrastructures nécessaires à l'authentification forte. Ils devront également améliorer la gestion des fraudes. Les consommateurs et les commerçants devront s'équiper et se former pour pouvoir utiliser l'authentification forte.

Les normes prévoient également des dérogations à l'authentification forte, pour éviter un trop grand bouleversement des façons de faire actuelles des consommateurs, des commerçants et des prestataires de services de paiement. L'autre raison de ces dérogations est qu'il peut exister d'autres mécanismes d'authentification tout aussi sûrs et sécurisés. Néanmoins, les prestataires de services de paiement qui voudront être exemptés de l'obligation de recourir à l'authentification forte devront d'abord appliquer des mécanismes de suivi des opérations afin d'évaluer l'ampleur du risque de fraude.

Tous les prestataires de services de paiement devront prouver que les mesures de sécurité sont mises en œuvre, testées et vérifiées. En cas d'opération de paiement frauduleuse, le consommateur pourra prétendre à un remboursement intégral.

Pour les opérations électroniques à distance, la sécurité sera renforcée au moyen d'un lien dynamique avec une opération en ligne d'un montant donné avec un commerçant donné. En cas de piratage de cette opération, l'information obtenue ne pourra pas être réutilisée par un fraudeur potentiel pour initier une opération similaire ou une autre opération.

Quand l'authentification forte du client deviendra-t-elle obligatoire?

Le recours à l'authentification forte deviendra obligatoire 18 mois après l'entrée en vigueur des normes techniques de réglementation, c'est-à-dire après leur publication au *Journal officiel de l'Union européenne*.

Cela donnera aux prestataires de services de paiement, notamment aux banques, suffisamment de temps pour adapter leur système de sécurité aux exigences accrues de sécurité définies par la DSP2.

Qu'en est-il de la sécurité des paiements effectués par les entreprises?

Les normes techniques de réglementation traitent également de la sécurité des paiements effectués par lots. En effet, la plupart des entreprises effectuent leurs paiements de cette manière, plutôt que un par un. Les nouvelles règles tiennent aussi compte de la communication *host-to-host* (connexion directe), dans le cadre de laquelle, par exemple, le système informatique d'une entreprise communique avec celui d'une banque pour envoyer des messages relatifs au paiement des factures. Les mécanismes de sécurité pour ce type de systèmes de communication peuvent être aussi efficaces que l'authentification forte du client. Par conséquent, si les autorités de surveillance nationales donnent leur

approbation, ils peuvent bénéficier d'une dérogation à l'obligation d'authentification forte.

L'authentification forte lorsque les consommateurs achètent et payent en ligne risque-t-elle de perturber le commerce électronique ?

La Commission souhaite favoriser le développement du commerce électronique en renforçant la confiance des consommateurs. Dans le même temps, elle souhaite réduire la fraude touchant les paiements en ligne, qui y sont particulièrement exposés. Il faut pour cela que le niveau de sécurité soit relevé, ce qui peut nécessiter que les acteurs du secteur adaptent leur système informatique ou leur modèle d'entreprise pour les rendre plus sûrs.

Les commerçants seront toujours en mesure d'appliquer l'analyse des risques aux opérations avec leurs clients. Cette méthode est souvent utilisée pour les paiements par carte. Les normes techniques de règlementation n'empêchent pas les commerçants de continuer à employer cette méthode. La DSP2 ainsi que les normes techniques de réglementation adoptées aujourd'hui ne concernent que les prestataires de services de paiement, dont les banques des consommateurs et celles des commerçants. Les commerçants eux-mêmes n'entrent pas dans le champ d'application des normes. Il appartiendra aux commerçants et à leurs prestataires de services de paiement de s'entendre sur la manière d'atteindre l'objectif de réduction de la fraude.

3. Communication sécurisée et standardisée

Comment fonctionnera la communication sécurisée et standardisée?

La DSP2 établit un cadre pour les nouveaux services liés aux comptes de paiement des consommateurs, tels que les services dits «d'initiation de paiement» et d'«information sur les comptes». Dans ce contexte, les normes techniques de réglementation définissent les exigences pour assurer une communication sécurisée et standardisée entre les banques et les sociétés de technologie financière («Fintech»).

Les consommateurs et les entreprises seront en mesure d'autoriser l'accès à leurs données de paiement à des tiers fournissant des services de paiement (PSP tiers). Ces tiers sont, par exemple, des prestataires de services d'initiation de paiement (PSIP) ou des prestataires de services d'information sur les comptes (PSIC). Les PSP tiers sont parfois des «FinTech», mais il peut également s'agir d'autres banques.

L'accès aux données, leur utilisation et leur traitement ne seront possibles qu'avec l'accord des clients. Les PSP tiers ne pourront pas accéder à des données du compte de paiement autres que celles ayant fait l'objet d'une autorisation expresse du client.

Les banques devront mettre en place un canal de communication qui permettra aux PSP tiers d'accéder aux données dont ils ont besoin. Ce canal permettra en outre aux banques et aux PSP tiers qui accéderont à des données de clients de s'identifier réciproquement et de communiquer à tout moment par une messagerie sécurisée.

Les banques pourront établir ce canal de communication en adaptant leur interface de services bancaires en ligne pour les clients. Elles pourront également choisir de créer une nouvelle interface spécifique, qui intégrera toutes les informations nécessaires pour les prestataires de services de paiement.

Par ailleurs, les règles précisent les mesures de sauvegarde d'urgence que les banques doivent mettre en place si elles décident de créer une interface spécifique (mécanismes dits «de secours»). L'objectif de ces mesures est d'assurer la continuité du service ainsi qu'une concurrence loyale sur ce marché.

Quels sont les critères d'une bonne interface de communication spécifique?

En vertu des normes techniques de réglementation, toutes les interfaces de communication, qu'elles soient spécifiques ou non, feront l'objet d'un essai de prototype de trois mois et d'un essai dans les conditions réelles du marché, de trois mois également. Ces essais permettront aux acteurs du marché d'évaluer la qualité des interfaces mises en place par les prestataires de services de paiement gestionnaires de comptes, y compris les banques.

Une bonne interface de communication spécifique devrait offrir en continu le même niveau de disponibilité et de performance que les interfaces mises à la disposition des consommateurs ou des entreprises pour l'accès direct à leur compte de paiement en ligne. En outre, une telle interface ne devrait pas créer d'obstacles à la fourniture des services d'initiation de paiement et des services d'information sur les comptes.

Les prestataires de services de paiement, y compris les banques, devront établir des indicateurs de performance clés et des objectifs de niveau de service transparents pour les interfaces de communication spécifiques, s'ils décident d'utiliser ce moyen. Ces indicateurs de performance devraient être au moins aussi stricts que ceux applicables aux plateformes de paiement et de services bancaires

en ligne utilisées par les clients.

La Commission promeut la création d'un groupe de marché, composé de représentants des banques, des prestataires de services d'initiation de paiement et de services d'information sur les comptes, et des utilisateurs de services de paiement. Ce groupe examinera la qualité des interfaces de communication spécifiques. Cette action s'inscrit dans le prolongement des travaux menés sur les services d'initiation de paiement par le Comité des paiements de détail en euros.

Les banques peuvent-elles être exemptées de l'obligation de prévoir un mécanisme de secours?

Oui. Elles peuvent en être exemptées à condition de mettre en place une interface de communication spécifique pleinement opérationnelle conforme aux critères de qualité définis par les normes techniques de réglementation. Les autorités nationales octroieront l'exemption aux banques au cas par cas, après avoir consulté l'ABE. Cette dernière doit veiller à ce que les autorités nationales évaluent la qualité des interfaces spécifiques selon des interprétations similaires. En effet, des divergences à cet égard nuiraient au bon fonctionnement du marché unique des paiements de détail.

Une autorité nationale peut révoquer l'exemption lorsqu'une interface de communication spécifique cesse, durant plus de deux semaines calendrier consécutives, de satisfaire aux critères de qualité définis par les normes techniques de réglementation. Dans ce cas, l'autorité nationale informe également l'ABE. L'autorité nationale veille également à ce que la banque mette en place un mécanisme automatisé de secours. Cette mise en place doit se faire dans les plus brefs délais et, en tout état de cause, dans les deux mois.

4. Protection des données à caractère personnel

Comment les données personnelles sont-elles protégées?

Les titulaires de compte peuvent exercer un contrôle sur la transmission de leurs données à caractère personnel tant au titre de la DSP 2 qu'au titre de la directive sur la protection des données (au titre du règlement général sur la protection des données à partir du 25 mai 2018). Aucun traitement de données ne peut avoir lieu sans le consentement exprès du consommateur. En outre, l'accès et le traitement par les PSP ne sont autorisés que pour les données à caractère personnel qui sont nécessaires à l'exécution de leurs services et pour lesquelles le consommateur a donné son accord.

La DSP 2 réglemente la fourniture de nouveaux services de paiement qui nécessitent l'accès aux données de l´utilisateur de services de paiement. Il peut s'agir par exemple de l'initiation d'un paiement au départ du compte du client, ou de la globalisation, à des fins de gestion des finances personnelles, d'informations relatives à un ou plusieurs comptes de paiement détenus auprès d'un ou de plusieurs PSP. Le consommateur ou la consommatrice qui souhaite bénéficier de ces nouveaux services de paiement devra les demander explicitement au prestataire concerné.

Les PSP doivent informer leurs clients de la manière dont leurs données seront traitées. Ils devront aussi respecter les droits des autres consommateurs en vertu des règles de protection des données, notamment le droit d'accès ou le droit à l'oubli. Tous les PSP (banques, établissements de paiement ou nouveaux prestataires) doivent respecter les règles de protection des données lorsqu'ils traitent des données à caractère personnel aux fins de services de paiement.

À quelles données les PSP peuvent-ils accéder par «screen scraping» et quelles données peuvent-ils utiliser?

La PSD 2 interdit aux PSP d'accéder à toute autre donné du compte de paiement du client que celles pour lesquelles le client a donné son autorisation explicite. Les clients devront consentir à l'accès, à l'utilisation et au traitement de ces données.

Avec les nouvelles règles, il ne sera plus permis d'accéder aux données du client par le recours aux techniques de «screen scraping» (capture de données d'écran), qui consistent à accéder aux données via l'interface client avec utilisation des données de sécurité du client. Par «screen scraping», les PSP peuvent accéder aux données des clients sans s'identifier davantage vis-à-vis de la banque.

Les banques devront mettre en place un canal de communication qui permette aux PSP d'accéder de manière conforme à la PSD 2 aux données dont ils ont besoin. Ce canal sera aussi utilisé pour permettre aux banques et aux PSP de s'identifier mutuellement lors de l'accès à ces données. Il leur permettra en outre de communiquer à tout moment par messages sécurisés.

Les banques peuvent établir ce canal de communication en adaptant l'interface de banque en ligne destinée à leurs clients. Elles peuvent aussi créer une nouvelle interface dédiée qui comportera toutes les informations nécessaires aux PSP concernés.

Les normes techniques de réglementation précisent les mesures de sauvegarde d'urgence que les banques devront mettre en place si elles décident de développer une interface dédiée. Une concurrence

équitable et la continuité des activités seront ainsi assurées pour les PSP.

5. Période de transition

Les PSP peuvent-ils continuer à recourir au «screen scraping» pendant la période de transition?

Une période de transition est prévue entre la date d'application de la PSD 2 (13 janvier 2018) et la date d'application des normes techniques de réglementation (18 mois après la publication de l'acte délégué au *Journal officiel de l'UE*). Les acteurs du marché des paiements ont besoin de cette période de transition pour mettre à niveau leurs systèmes de sécurité des paiements afin qu'ils répondent aux exigences définies dans ces normes.

Cela signifie que les dispositions de la PSD 2 sur l'authentification forte du client et sur la communication sécurisée, qui sont directement précisées dans les normes techniques de réglementation, ne s'appliqueront pas immédiatement. En d'autres mots, l'application des mesures de sécurité prévues aux articles 65, 67 et 97 de la PSD 2 est reportée jusqu'à ce que ces normes entrent en application. Cependant, les dispositions des articles 65, 67 et 97 qui ne dépendent pas des normes s'appliqueront à partir du 13 janvier 2018.

L'application plus tardive des normes techniques de réglementation ne devrait pas créer de difficultés pour la fourniture de services de paiement existants par les acteurs du marché qui exerçaient des activités dans les États membres avant le 13 janvier 2016. L'article 115, paragraphe 5, de la PSD 2 assure la continuité de ces services. Ces PSP devraient néanmoins demander dès que possible l'agrément nécessaire en vertu de la PSD 2 à leur autorité nationale.

Les nouveaux prestataires qui souhaitent fournir des services d'initiation de paiement ou des services d'information sur les comptes doivent obtenir l'agrément pertinent pour entrer sur le marché pendant la période de transition.

MEMO/17/4961

Personnes de contact pour la presse:

Vanessa MOCK (+32 2 295 61 94)
Letizia LUPINI (+32 2 295 19 58)

Renseignements au public: Europe Direct par téléphone au 00 800 67 89 10 11 ou par courriel