DSP2: vers une sécurisation ou de nouveaux risques systémiques?

Contact: Marie-Agnès NICOLET
Présidente de Regulation Partners
marieagnes.nicolet@regulationpartners.com
06 58 84 77 40

Contexte

La révision de la Directive Services de Paiement (DSP2)

Le **24 juillet 2013**, la Commission européenne a publié un **paquet législatif** comprenant, entre autres, une **proposition de révision de la directive sur les services de paiement** (DSP2) afin de :

- prendre en compte les **évolutions technologiques**,
- **Prendre en compte les nouveaux usages apparus sur le marché des paiements** depuis l'adoption de la DSP1 en 2007 (croissance continue du e-commerce, développement du m-commerce...),
- assurer un **haut niveau de sécurisation** des moyens de paiement,
- **maintenir la confiance des usagers** des établissements bancaires
- Favoriser la concurrence (apparition de nouveaux acteurs).

PSIC et PSIP

Des prestataires de service d'information sur les comptes :

Le point 16 de l'article 4 de la directive DSP2 en donne la définition suivante :

« Service en ligne consistant à fournir des informations consolidées concernant un ou plusieurs comptes de paiement détenus par l'utilisateur de services de paiement soit auprès d'un autre prestataire de services de paiement, soit auprès de plus d'un prestataire de services de paiement ».

Prestataire de service d'initiation de paiement

Le point 17 de l'article 4 de la directive DSP2 en donne la définition suivante :

« Service consistant à initier un ordre de paiement à la demande de l'utilisateur de services de paiement concernant un compte de paiement détenu auprès d'un autre prestataire de services de paiement »

Comment assurer la sécurité nécessaire au bon fonctionnement des moyens de paiements puisque ces nouveaux entrants proposent des services qui nécessitent l'accès aux données bancaires de leurs clients ?

Droits et obligations liés à la prestation et à l'utilisation de services de paiement

Obligations de l'utilisateur de services de paiement, liées aux instruments de paiement et aux données de sécurité personnalisées :

- L'utilisateur a un usage conforme aux conditions préalablement définies, et qui se doivent d'être non discriminatoires, objectives et proportionnées.
- Quand l'utilisateur a connaissance de la perte - vol - détournement - utilisation non autorisée de l'instrument de paiement, il en informe sans tarder le prestataire, afin de préserver la sécurité de ses données personnelles

Obligations du PSP, liées aux instruments de paiement :

- Le PSP s'assure que les données personnelles ne sont pas accessibles à d'autres parties que l'utilisateur du service de paiement
- Le PSP s'abstient d'envoyer tout instrument de paiement non sollicité par l'utilisateur, sauf remplacement
- Le PSP fournit à l'utilisateur de services de paiement la possibilité de procéder à la notification en cas de perte / vol / détournement / utilisation non autorisée de l'instrument
- Le PSP empêche toute utilisation de l'instrument après notification de perte / vol / détournement / utilisation non autorisée par l'utilisateur de service de paiement
- Le PSP supporte le risque lié à l'envoi, à l'utilisateur de service de paiement, d'instrument de paiement ou de toute données personnelle relative à celui-ci.

Droits et obligations liés à la prestation et à l'utilisation de services de paiement

Article L.133-44-I Code monétaire et financier – Authentification forte

L'authentification forte s'applique lorsque le payeur :

- Accède à son compte de paiement en ligne
- Initie une opération de paiement électronique
- Exécute une opération par le biais d'un moyen de communication à distance, susceptible de comporter un risque de fraude en matière de paiement ou toute autre utilisation frauduleuse

❖ Appliquer une authentification forte du client comportant des éléments qui établissent un lien dynamique entre l'opération, le montant et le bénéficiaire donnés.

❖ Exécute une action grâce à un moyen de communication à distance, susceptible de comporter un risque de fraude en matière de paiement ou toute autre utilisation frauduleuse.

Droits et obligations liés à la prestation et à l'utilisation de services de paiement

L'authentification forte du payeur :

Une authentification reposant sur l'utilisation de **deux éléments** ou plus appartenant aux **catégories «connaissance», «possession» et «inhérence»** (quelque chose que l'utilisateur est) et indépendants en ce sens que la compromission de l'un ne remet pas en question la fiabilité des autres, et qui est conçue de manière à protéger la confidentialité des données d'authentification

1. **Connaissance** : quelque chose que seul l'utilisateur connaît (*comme un mot de passe, un code d'identification personnel, ou un « code PIN », etc.*)

2. **Possession** : quelque chose que seul l'utilisateur possède (*comme un «token », un téléphone mobile, une carte à micro-processeur ou « carte à puce » etc.*)

3. **Inhérence** : quelque chose qui est liée à la personne elle-même de l'utilisateur (*une caractéristique biométrique telle que l'empreinte digitale ou la voix par exemple*)

Les exemptions envisagées par la version finale des RTS sont :

- Les paiements effectués sur des terminaux de paiement autonomes (par exemple ceux utilisés dans les transports en commun ou les parkings).
- Une analyse des risques relatifs aux transactions : Niveau prédéfini de fraude :
  - La méthodologie d'analyse de risques est strictement encadrée par l'article 16 des RTS.
  - Cette analyse devra être menée par la banque du payeur en temps réel :
    - **Collecte et analyse des données :** données de navigation, données liées à la transaction, données comportementales, données contextuelles…. Autant de paramètres qui permettent après neutralisation des faux positifs de révéler le caractère potentiellement frauduleux ou non d'une transaction.
    - **Parmi les critères importants** : la vélocité (plusieurs transactions réalisées en peu de temps sur des zones éloignées), l'adresse de livraison, ou encore le type de produit, l'e-réputation, etc.
  - Seules les banques disposant d'un taux de fraude égal ou inférieur au taux de référence défini à l'article 16 des RTS pourront se prévaloir de ce type d'exemption.

Standards Techniques Réglementaires (RTS)

- **L'exemption ne pourra être appliquée qu'aux transactions dont le montant sera en dessous de seuils également définis à l'article 16, qui varient entre 100€ et 500€, et qui dépendent du taux de fraude de la banque émettrice de la carte pour le paiement par carte sur l'instrument de paiement utilisé (virement et paiement par carte)**
  - Si l'analyse conclut à un risque faible, l'exemption à l'authentification forte pourra s'appliquer.
  - Par exemple : exemption à l'application de l'authentification forte pour les transactions par carte allant jusqu'à 500€ pour les banques qui ont un taux de fraude sur le paiement à distance par carte inférieur ou égal à 0,01%. En revanche, exemption possible pour les transactions de 250€ maximum, si la banque a un taux de fraude sur le paiement à distance par carte entre 0,01% et 0,06%.
- **L'exemption relative à l'analyse des risques d'une transaction est liée à un niveau prédéfini de fraude et est assujettie à une clause de révision, 18 mois après la date d'application des RTS.**

Dernières évolutions réglementaires en France

Ordonnance n°2017-1252 du 9 août 2017
Transposition de la Directive 2015-2366

Rappel

La **directive n° 2015/2366** comporte des dispositions relatives à quatre grandes thématiques :

- la première aux conditions d'exercice des ***prestataires de services de paiement*** ;
- la seconde aux droits et obligations des ***utilisateurs et des prestataires de services de paiement*** ;
- la troisième aux exigences en matière ***d'information relatives aux services de paiement*** ; et
- la quatrième aux exigences de ***sécurité renforcées pour les paiements électroniques et la protection des données financières des consommateurs*.**

- **L'Ordonnance n°2017-1252 du 9 août 2017 portant transposition de la directive 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur** publiée au Journal officiel de la République française **le 10 août 2017**.
- La présente ordonnance modifie le code monétaire et financier et **s'accompagne d'un décret en Conseil d'Etat, d'un décret simple et de cinq arrêtés**.

Ordonnance n°2017-1252 du 9 août 2017

S'agissant des conditions d'exercice des établissements de paiement:

- Les **dispositions du CMF** relatives aux **conditions d'octroi de leur agrément sont complétées.**
- La **protection des fonds des utilisateurs** de services de paiement **reste obligatoire** pour l'ensemble de ces établissements par le biais d'un **cantonnement des fonds collectés** pour l'exécution d'opérations de paiement.
- Pour les **établissements dont la moyenne mensuelle de la valeur totale des opérations de paiement ne dépasse pas 3 millions d'euros, un agrément simplifié est ouvert**.
- Les **exigences prudentielles plus favorables** qui préexistaient sont **maintenues,** et les **informations requises dans le cadre du dossier de demande d'agrément sont allégées.**
- En matière de supervision des activités transfrontalières, la directive organise une **procédure de coopération entre les autorités compétentes** et **renforce les pouvoirs de l'Etat membre d'accueil**.
- Il est désormais permis à l'ACPR de **prendre des mesures conservatoires** en cas **d'urgence à l'égard des établissements agréés dans un autre Etat membre de l'Union européenne** et **exerçant leur activité en France,** lorsqu'une **action immédiate est nécessaire** pour **contrer une menace grave pour les intérêts collectifs des utilisateurs de services de paiement.**

Ordonnance n°2017-1252 du 9 août 2017

S'agissant des droits et obligations des utilisateurs et des prestataires de services de paiement :

- La présente ordonnance introduit des dispositions nouvelles destinées **à renforcer les droits des utilisateurs** :

- **Réduction de leur responsabilité de 150 euros à 50 euros en cas de paiements non autorisés,** c'est-à-dire de paiements consécutifs à un vol, une perte ou un détournement de l'instrument de paiement.

- **Les utilisateurs doivent également être informés sans délai des incidents opérationnels et de sécurité majeurs** - c'est-à-dire des incidents affectant le fonctionnement de l'établissement ou la sécurité de l'opération de paiement - lorsque l'incident est susceptible d'avoir des répercussions sur leurs intérêts financiers.

- **Enfin, les utilisateurs de services de paiement doivent être informés des procédures de réclamation existantes, ainsi que des procédures de règlement extrajudiciaire en cas de litige.**

Ordonnance n°2017-1252 du 9 août 2017

S'agissant des exigences en matière d'information relatives aux services de paiement :

- Les **prestataires de services de paiement** fournissant les services d'information sur les comptes ou les services d'initiation de paiement sont ainsi **tenus de fournir l'ensemble des informations requises relativement aux opérations de paiement.**

Les exigences de sécurité pour les paiements électroniques et la protection des données financières des consommateurs sont renforcées:

- **L'authentification forte du client**, consistant à vérifier l'identité du payeur lors de l'opération de paiement, par exemple **en renseignant un code additionnel**, **devient obligatoire** en application de cette directive suivant des conditions précisées par l'Autorité bancaire européenne.

- **La Banque de France et l'ACPR** sont par ailleurs **informées sans délai respectivement des incidents opérationnels majeurs et des incidents de sécurité majeurs.**

Arrêté du 31 août 2017 modifiant l'arrêté du 29 juillet 2009

Arrêté du 31 août 2017 modifiant l'arrêté du 29 juillet 2009

Relatif aux relations entre les prestataires de services de paiement et leurs clients en matière **d'obligations d'information des utilisateurs de services de paiement** et précisant les principales stipulations devant figurer dans **les conventions de compte de dépôt et les contrats-cadres de services de paiement**

- Précise les informations à fournir/ mettre à disposition par le PSP immédiatement après avoir initié un ordre de paiement au payeur ou, le cas échéant au bénéficiaire

- Publié au Journal officiel de la République française le 2 septembre 2017.
- L'arrêté entre en vigueur le 13 janvier 2018 .

- Précise les informations que le PSP doit fournir ou mettre à la disposition pour la fourniture des services de paiement, avant que l'utilisateur de services de paiement ne soit lié par un contrat relatif à une opération de paiement isolée ou à la fourniture d'un service de paiement ne relevant pas d'une convention de compte de dépôt ou d'un contrat-cadre de services de paiement

- **<u>Précise les informations contenues dans les conventions de compte de dépôt et les contrats cadres concernant les opérations de paiement</u>** :

  - Sur le prestataire de services de paiement
  - Sur l'utilisation d'un service de paiement
  - Sur les frais, les taux d'intérêt et les taux de change
  - Sur la communication entre l'utilisateur et le prestataire de services de paiement
  - Sur les mesures de protection et les mesures correctives
  - Sur la modification et la résiliation du contrat
  - Sur les comptes joints
  - Sur les recours

Arrêté du 31 août 2017 modifiant l'arrêté du 29 juillet 2009

Le contrat de dépôt ou le contrat-cadre comporte les <u>informations suivantes</u> lorsqu'il s'agit d'opérations de paiement réalisées par des PSP

Des informations relatives aux comptes joints
notamment, les modalités de fonctionnement et de clôture d'un compte de paiement joint

Sur les recours : le droit applicable au contrat et la juridiction compétente, les voies de réclamation et recours extrajudiciaires

Sur la modification et la résiliation du contrat

Des informations sur les frais, les taux d'intérêt et les taux de change

Des informations relatives au PSP:

- le nom, l'adresse du siège social, toutes les adresses à prendre en compte pour la communication avec le PSP (*y compris l'adresse de courrier électronique*), etc.
- Les coordonnées des autorités de contrôle compétentes et les informations permettant à l'utilisateur de s'assurer de l'habilitation du PSP, (*y compris les informations permettant de consulter la liste des PSP*);

Sur la communication entre l'utilisateur et le PSP:

- Les moyens de communication,
- Les modalités et la fréquence selon lesquelles les informations sont fournies ou mises à disposition,
- La/les langues dans lesquelles le contrat est conclu,
- La mention du droit de l'utilisateur de services de paiement de recevoir les termes contractuels du contrat,
- Les finalités des traitements de données mis en œuvre par le PSP, les destinataires des informations, le droit de s'opposer à un traitement des données à des fins de prospection commerciale ainsi que les modalités d'exercice du droit d'accès aux informations concernant le client

Arrêté du 31 août 2017 modifiant l'arrêté du 29 juillet 2009

regulation partners

Le contrat de dépôt ou le contrat-cadre comporte les informations suivantes lorsqu'il s'agit d'opérations de paiement réalisées par des PSP

Sur l'utilisation d'un service de paiement

- Une description des principales caractéristiques du service de paiement à fournir
- Les informations précises ou l'identifiant unique que l'utilisateur de services de paiement doit fournir aux fins de l'initiation ou de l'exécution correcte de son ordre de paiement;
- La forme et la procédure pour donner le consentement à l'initiation ou à l'exécution d'une opération de paiement et pour retirer ce consentement,
- Dans le cas d'instruments de paiement liés à une carte cobadgés, les droits de l'utilisateur de services de paiement
- Une information sur le moment de réception de l'ordre de paiement et l'éventuel délai limite établi par le PSP
- Les obligations de confidentialité à la charge du prestataire de services de paiement,
- Le sort du compte de paiement au décès du ou de l'un des titulaires du compte de paiement
- Les modalités de procuration, la portée d'une procuration et les conditions et conséquences de sa révocation;
- La possibilité, si elle existe, de convenir de limites de dépenses pour l'utilisation de l'instrument de paiement
- Le délai d'exécution maximal au cours duquel le service de paiement doit être fourni;

Arrêté du 31 août 2017 modifiant l'arrêté du 3 novembre 2014

Nouvel article 249-1

« **Art. 249-1**. – En ce qui concerne les incidents majeurs au sens de l'**article L. 521-10 du code monétaire et financier**, les dirigeants effectifs informent sans retard injustifié l'ACPR de tout incident opérationnel et la Banque de France de tout **incident de sécurité**.»

Incident de sécurité

Définition

« Un événement ou une série d'événements imprévus résultant de processus internes inadaptés ou défaillants ou d'évènements extérieurs affectant la disponibilité, l'intégrité, la confidentialité et la continuité des systèmes d'information et de communication et/ou les informations utilisées pour la fourniture de services de paiement. Ceci inclut les incidents provenant de cyber-attaque ou de la non pertinence des mesures de sécurité physique. »

REPORTING DES INCIDENTS

Orientations de l'EBA du 19/12/2017 sur la notification des incidents majeurs en vertu de la directive UE 2015/2366 (DSP2)

Incidents majeurs

Evaluation des impacts des incidents

Notification des incidents majeurs à l' autorité compétente

Notification initiale envoyée dans les 4 heures suivant la détection de l'incident opérationnel ou de sécurité majeur

Notification finale lorsque l'analyse des causes a été réalisée

Modèle de notification pour les PSP.

RISQUES OPERATIONNELS

Orientations de l'EBA du 12/01/2018 relatives aux mesures de sécurité pour les risques opérationnels et de sécurité liés aux services de paiement dans le cadre de la directive DSP2

Diagnostic à réaliser

- Gouvernance
- Evaluation des risques
- Mesures préventives
- Détection
- Continuité d'activité
- Tests des mesures de sécurité
- Connaissance des situations et formation continue
- Gestion des relations avec les utilisateurs des services de paiement

Délai de traitement des réclamations – Ordonnance 9 août 2017

Ordonnance 9 août 2017 – Section 16 « *Traitement des réclamations* »

« **Art. L. 133-45.-** Les prestataires de services de paiement mettent en place et appliquent des procédures destinées au traitement des réclamations des utilisateurs de services de paiement portant sur le respect des dispositions de la section 5 du chapitre II du titre Ier du livre Ier, du chapitre III du titre III du livre Ier, du chapitre IV du titre Ier du livre III et du chapitre Ier du titre II du livre V.

« Ces procédures sont accessibles dans une des langues officielles de l'Etat membre concerné ou dans une autre langue si le prestataire de services de paiement mentionné à l'alinéa premier et l'utilisateur de services de paiement en sont convenus ainsi.

« Les prestataires de services de paiement mentionnés à l'alinéa premier répondent sur support papier ou, s'ils en sont convenus ainsi avec l'utilisateur de services de paiement, sur un autre support durable, aux réclamations des utilisateurs de services de paiement.

« Cette **réponse aborde tous les points soulevés dans la réclamation** et est **transmise dans les meilleurs délais** et au plus tard dans les **quinze jours ouvrables suivant la réception de la réclamation**.

« Dans des situations exceptionnelles, **si une réponse ne peut être donnée dans les quinze jours ouvrables pour des raisons échappant au contrôle du prestataire de services de paiement, celui-ci envoie une réponse d'attente motivant clairement le délai complémentaire nécessaire pour répondre à la réclamation et précisant la date ultime à laquelle l'utilisateur de services de paiement recevra une réponse définitive**. En tout état de cause, l'utilisateur de services de paiement reçoit une réponse définitive **au plus tard trente-cinq jours ouvrables suivant la réception de la réclamation.**