Traitement des données personnelles

Annexe Opérationnelle Payline

Référence	:	SEC/DCP/Payline/20190131-01
Date	:	05/06/2019
Version/Édition	:	2A
Classification	:	C0 (Public)

TABLE DES MATIERES

1 Introduction

Dans le cadre du contrat de prestations de services « Payline » entre le Client et Monext, Monext réalise un certain nombre de traitements pour le compte du Client.

Ces traitements peuvent concerner des données à caractère personnel telles que définies par le Règlement Général sur le Données Personnelles (RGPD) 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.

2 Description des traitements

Payline est une solution de paiement sécurisée en ligne. Elle permet aux commerçants ayant une activité de vente à distance de gérer des paiements par cartes bancaires et autres moyens de paiement alternatifs, *de gérer un portefeuille de moyens de paiements*, et enfin de *lutter contre la fraude*.

En termes d'interfaces techniques, l'intégration de Payline avec le site de commerce en ligne du Commerçant peut être effectuée de 2 manières différentes :

- Les données à caractère personnel sont collectées par le site Commerçant du Client et transmises à Payline pour traitement : **collecte indirecte**.
- Les données à caractère personnel sont collectées, pour le compte du Client, par des pages web fournies par Payline qui sont intégrées dans le site web du Commerçant : **collecte directe**.

Certaines données sont fournies par le Moyen de Paiement lors du processus de paiement.

2.1.1 Traitement «Gérer des paiements»

Accepter des paiements

Le traitement qui permet à un Commerçant d'accepter des paiements consiste à :

- Faire une demande d'autorisation de débit auprès du moyen de paiement (ou la banque acquéreur de ce moyen de paiement). Lors de cette demande, Payline transmet différentes données personnelles dont des données de paiement (Par exemple : un numéro de carte bancaire) dans le but de permettre au moyen de paiement d'évaluer le risque et de communiquer son accord pour le paiement.
- Confirmer le débit des transactions d'autorisation acceptées. Pour réaliser cette confirmation, Payline effectue, en fonction des moyens de paiement, une des actions suivantes :
    - une remise en banque, envoyée quotidiennement par fichier à destination d'une banque acquéreur, de l'ensemble des transactions à créditer ou à débiter pour le compte de commerçants ;
    - une demande de confirmation de débit unitaire pour chaque transaction d'autorisation acceptée.

- Envoyer le ticket de paiement par email au consommateur et au commerçant.

Payline propose plusieurs modes de paiement. La durée de traitement et de stockage des données de la transaction diffèrent comme le précise les cas suivants :

1. **Paiement à la commande** : la confirmation du débit est réalisée à J+1 de la transaction hors jour non ouvré.
2. **Paiement différé ou à l'expédition** : Ce type de paiement est majoritaire dans Payline car les Commerçants appliquent la loi Chatel qui impose le débit à l'expédition d'une commande. La confirmation du débit est réalisée dans la majorité des cas entre J+1 et J+11 de la transaction hors jour non ouvré (cas Visa/MasterCard à J+30).
3. **Paiement en N fois** : Ce type de paiement s'appuie sur l'enregistrement de la carte dans un portefeuille virtuel Payline. Il s'agit d'enregistrer les données de la carte bancaire (dans le respect des exigences PCI DSS) pendant le temps nécessaire au traitement des N échéances. N étant précisé par le Commerçant lors de la demande de paiement et communiqué au consommateur avant sa confirmation de paiement et à réception du ticket de paiement par email.
4. **Paiement par abonnement** : Ce type de paiement s'appuie sur l'enregistrement de la carte dans un portefeuille virtuel Payline. Il s'agit d'enregistrer les données de la carte bancaire (dans le respect des exigences PCI DSS) pendant le temps nécessaire au traitement de l'abonnement ou pendant la durée de validité de la carte. La durée de l'abonnement peut être précisée par le Commerçant lors de la demande de paiement.
5. **Paiement en 1 clic** : Ce type de paiement s'appuie sur l'enregistrement de la carte dans un portefeuille virtuel Payline. Il s'agit d'enregistrer les données du moyen de paiement pendant la durée de validité de la carte + 2 mois.

Durée de conservation des données ***: 13 mois***.

Rembourser des paiements

Le traitement qui permet à un Commerçant de rembourser des paiements consiste à :

- **Demander le remboursement** des transactions d'autorisation encaissées. Pour réaliser cette demande, Payline effectue, en fonction des moyens de paiement, une des actions suivantes :
  - une remise en banque, envoyée quotidiennement par fichier à destination d'une banque acquéreur, de l'ensemble des transactions à débiter pour le compte de commerçants ;
  - une demande de remboursement unitaire pour chaque transaction d'autorisation acceptée.
- **Envoyer le ticket de remboursement** par email au consommateur et au commerçant.

Le traitement est réalisé entre J et J+1 à partir de la demande du Commerçant hors jour non ouvré.

Durée de conservation des données : ***13 mois***.

Gestion du commerçant

Le Commerçant désigne certains de ses collaborateurs ayant droit d'accéder au back-office Payline ou pour être destinataire d'informations, d'alertes ou de reporting liés aux prestations Payline.

Le Commerçant communique les informations d'identifications à Monext qui assure la gestion des connexions et des utilisateurs.

De plus, le Commerçant désigne certains de ses collaborateurs pouvant accéder au Service Clients Payline. Les événements et les relations entre ces collaborateurs et le Service Clients Payline sont consignés en utilisant une plateforme Cloud Zendesk.

Durée de conservation des données : ***durée du contrat entre le Commerçant et Payline + 24 mois***.

Reporting et réconciliation

Payline propose 3 types de rapports accessibles en ligne via le backoffice ou via un transfert de fichier sécurisé et automatisé, ou envoyé par mail au Commerçant :

Le rapport des transactions

Ce rapport permet d'obtenir l'activité du commerçant.

La liste contient les transactions réalisées de type abandonnées, acceptées ou refusées.

Ces transactions contiennent des informations du consommateur, du moyen de paiement, de la commande et de la transaction monétique.

Payline sélectionne les données dans la base de données, génère un fichier et le met à disposition du commerçant par l'intermédiaire d'une passerelle de transfert. Il est supprimé dès qu'il est récupéré. Il est gardé pendant 45 jours maximum.

Durée de conservation des données : ***24 mois pour les données contenues dans les rapports des transactions.***

Le rapport des paiements

Ce rapport permet d'avoir une vision de l'ensemble des paiements envoyés en banque. La liste des opérations contient des opérations de crédit, de débit, des remboursements, des impayés et des opérations compensées. Payline intègre les journaux des relevés bancaires et impayés. Il permet la gestion de l'activité financière du commerçant. Il contient les informations :

- montant et nombre de débit, crédit et impayé par Commerçant (pour un groupe), point de vente et moyen de paiement ;
- toutes les transactions concernées avec uniquement des informations personnelles tronquées (exemple : n° de carte masqué).

On ne trouve aucune donnée à caractère personnel dans ce rapport.

Durée de conservation des données : ***13 mois pour les données contenues dans les rapports des paiements.***

Les rapports statistiques

Ces rapports aident l'analyse et le pilotage de l'activité et de la stratégie du commerçant.

Ces rapports donnent sont regroupés en quatre catégories : performance, risque, optimisation et finance.

L'outil de Business Intelligence sélectionne les données concernant le commerçant, calcule les indicateurs demandés et les met à disposition sur l'interface commerçant ou, sur demande, génère des fichiers envoyés au commerçant.

On ne trouve aucune donnée à caractère personnel dans ces rapports.

2.1.2 Gérer un portefeuille de moyens de paiements

Principe

Payline offre la possibilité de gérer les portefeuilles virtuels pour le compte des Commerçants.

Un portefeuille virtuel est destiné à conserver les données de paiement des payeurs en vue de les fidéliser et de leur éviter lors d'une prochaine transaction une nouvelle saisie de leurs données de paiement.

Un portefeuille virtuel sauvegarde les données monétiques : numéro de carte, date d'expiration et éventuellement les données d'identification du titulaire (ex : nom, prénom)

Plusieurs moyens de paiement peuvent être enregistrés dans un même portefeuille :

Création

Payline permet la création d'un portefeuille via les interfaces suivantes :

- les pages de paiement : lors d'une demande de paiement, le Commerçant précise que le moyen de paiement doit être enregistré dans un portefeuille. Dans ce cas, une fois la demande de paiement traitée, Payline crée un portefeuille avec les informations du client : nom, prénom et moyen de paiement,
- les pages web de création d'un portefeuille : le Commerçant invite le payeur à pré-enregistrer ses données de paiement pour lui faciliter ses prochains achats. Le Commerçant redirige le client sur les pages web de création d'un portefeuille. Le client enregistre ses moyens de paiement et Payline enregistre le portefeuille.
- L'interface directe commerçant (webservices)

Gestion du portefeuille virtuel

Les pages de paiement Payline, l'API webservice et le Centre d'Administration Payline permettent de gérer un portefeuille virtuel.

Les pages de paiement disposent des fonctions d'affichage et de mise à jour d'un portefeuille.

En plus de ces fonctions, l'API webservice permet de désactiver/réactiver un portefeuille complet ou uniquement un moyen de paiement.

Le Centre d'Administration (back office Payline) permet également aux utilisateurs autorisés du Commerçant de rechercher, visualiser, activer/désactiver et mettre à jour un portefeuille ainsi que les moyens de paiements qu'il contient.

Gestion du consentement

En cas de collecte directe des données, Payline fournit les outils techniques permettant au Commerçant de remplir ses obligations concernant le consentement.

Sécurisation des paiements par portefeuille virtuel

L'enregistrement d'une carte bancaire dans le portefeuille est systématiquement contrôlé par une demande d'information ou une transaction d'autorisation à 1 euro (qui est annulée juste ensuite, donc sans paiement réel). Ces opérations sont invisibles pour le client.

Les cartes mises en opposition sont automatiquement désactivées du portefeuille et une notification est envoyée au Commerçant par message de serveur à serveur.

Lors de la demande de paiement, des contrôles de sécurité (demande du cryptogramme visuel ou activation du 3D Secure) peuvent être activés par le Marchand en fonction de ses propres critères : modification de l'adresse de livraison, pays de l'adresse IP du client, récence d'achat, …

Durée de conservation des données : date de fin de validité du moyen de paiement + ***2 mois***.

2.1.3 Lutter contre la fraude

Le traitement de lutte contre la fraude consiste à analyser chaque transaction pour en déterminer le risque de fraude et, en fonction du résultat, déclenche une authentification 3DSecure, met la transaction en attente pour une analyse manuelle ou refuse la transaction.

Les listes

Le module de lutte contre la fraude utilise un système de listes dont le principe de fonctionnement est le suivant :

Les listes, propres à chaque Commerçant, regroupent des données composant une transaction qui permettent de déterminer si cette dernière comporte un risque plus ou moins élevé. La liste noire correspond à un risque très fort, la liste grise à un risque élevé, la liste de nouveaux clients à un risque modéré et les listes blanches et de clients connus à un risque faible. Seule la liste noire réalise un refus systématique. Les autres listes permettent d'adapter le nombre de contrôle et les seuils de ces contrôles.

L'ajout et ou la suppression d'éléments en liste peut être réalisé de manière manuelle (API ou backoffice) par le Commerçant ou automatique en fonction d'une suspicion de fraude ou d'une fraude avérée. Nous prenons soin de ne jamais mettre le consommateur dans une situation de blocage et encore moins de façon permanente. Ainsi une suspicion de fraude peut donner lieu à une mise en liste grise temporaire uniquement.

Les éléments suivants peuvent être ajoutés dans une liste : identifiant client, adresse email, numéro de téléphone, numéro de carte bancaire, compte acheteur, adresse IP, plage d'adresse IP, domaine de l'adresse email, pays émetteur de la carte, pays de l'adresse IP, nom du client, plage de BIN, et le type de carte.

Ces éléments sont automatiquement supprimés lorsque leur durée de stockage est dépassée ou que le Commerçant en demande la suppression (API ou backoffice).

Un rapport statistique est communiqué régulièrement au Commerçant dans le but de vérifier la pertinence d'un élément en liste et le cas échéant de retirer l'élément de la liste concernée.

Les règles

De plus, pour effectuer un contrôle du risque, le module anti-fraude utilise un système de règle dont le principe de fonctionnement est le suivant :

Une règle vérifie la valeur d'un composant de la transaction avec une valeur fixe ou une liste de valeur. Par exemple, la règle sur le montant maximum vérifie que le montant de la transaction est inférieure au seuil définit par le Commerçant dans la règle.

Dans le cas où la valeur dépasse le seuil, une action est réalisée :

- « aucune action »
- « déclencher 3DSecure »
- « demande analyse manuelle »
- « refuser la transaction »

Un contrôle peut regrouper plusieurs règles. Par exemple, contrôler le montant de la transaction et le pays d'origine de la carte. On parle alors d'une règle composée.

La liste des règles disponibles est : Type d'appareil, Résultat 3DSecure, Montant minimum, Montant maximum, Plage Horaire, Montant cumulé par client, Nb de transaction par client, Montant cumulé par client, Nb de transaction par moyens de paiement, Montant cumulé par adresse IP, Nb de transaction par adresse IP, Contrôle la valeur d'une donnée propre au Commerçant transmise lors de la transaction, Cohérence entre le pays du moyen de paiement et le pays de l'adresse IP, Nb de cartes utilisées par client, Nb de cartes partagées entre client, Nb de e-wallet utilisés par client, Nb de e-wallet partagés entre client, Ancienneté du compte client, Utilisation d'une nouvelle carte, Pays de l'adresse IP, Pays du moyen de paiement, Type de carte (carte virtuelle).

Un rapport statistique est communiqué régulièrement au Commerçant dans le but de vérifier la pertinence des contrôles appliqués et le cas échéant de modifier ou retirer le contrôle concerné.

Les alertes

Dans l'objectif de tester la pertinence de nouvelles règles ou de contrôler des cas à la marge, un système d'alerte permet d'informer le Commerçant par email ou par API qu'un cas nécessite son action.

Une alerte peut être déclenchée par n'importe quelle règle ou lors de la réception d'un évènement propre au moyen de paiement : mise en opposition de carte, fraude détecté chez le moyen de paiement après une autorisation ou réception d'un impayé.

Une alerte regroupe les informations suivantes visant à communiquer au destinataire toutes les informations utiles pour une prise de décision rapide sur la transaction. Les informations spécifiques sur la transaction concernent l'historique sur les 20 derniers jours du client, du moyen de paiement et de l'appareil utilisé pour payer. Ces informations sont cloisonnées et ne concernent que l'activité du consommateur chez le Commerçant concerné.

Les étapes du traitement sont les suivantes :

- Déterminer le modèle risque à appliquer pour la transaction : Il s'agit de déterminer si un des composants de la transaction est en liste noire, liste grise, liste blanche, liste des clients connus ou liste des nouveaux clients. Par défaut le modèle standard correspond à la liste de nouveaux clients.
- Exécuter les contrôles définis pour le modèle de risque déterminé et appliquer l'action correspondante. L'ensemble des contrôles est réalisé, qu'ils déclenchent ou non une action. L'action la plus « forte » sera appliquée en respectant l'ordre suivant : « aucune

action », « demande analyse manuelle », « déclencher 3DSecure », « refuser la transaction ».

- Emettre une alerte en temps réel dans le cas où une règle la déclenche ou à posteriori dans le cas où un évènement se produit.

Le processus d'identification du 3D Secure avec le MPI

Payline propose d'utiliser le dispositif 3DSecure lorsqu'une transaction est suspectée frauduleuse.

Lorsque l'action 3DSecure est déclenchée, le consommateur est prévenu qu'il va devoir s'authentifier auprès de sa banque afin de poursuivre son paiement. Payline route automatiquement la transaction sur le contrat 3D Secure afin de différencier les flux « garantis » ou non.

Le commerçant réalise une demande de vérification d'enrôlement à Payline, Payline contacte le 3DS server MODIRUM. Le dialogue d'authentification commence, il se décompose en 2 échanges :

1) Un premier échange vérifie sur les Directory Serveurs VISA, MASTERCARD, CB, AMEX, que la carte du porteur fait partie du programme 3-D Secure (porteur dit «enrôlé»).
2) Si la carte fait partie du programme 3-D Secure, un deuxième échange redirige le porteur vers le site d'authentification de la banque émettrice de la carte.

Ces messages assurent « le transfert de responsabilité » du paiement.

Durée de conservation des données : ***13 mois***

Le processus d'identification du matériel avec la règle « d'Ubiquité digitale »

Avec l'option de LCLF avancée, Payline propose des règles basées sur la signature du matériel utilisé par l'internaute

La finalité de cette règle d'ubiquité est de repérer qu'une même machine connectée (ordinateur, téléphone portable) est utilisée pour faire plusieurs transactions en apparence sans lien entre elles.

Elle est activée lorsque le client de Payline choisit cette option au niveau de son contrat.

Elle permet ainsi de détecter d'éventuelles fraudes, là où le fraudeur aurait modifié les paramètres comme son adresse email ou encore sa carte bancaire.

=> Identifier une source unique à l'origine de transactions hétérogènes ne pouvant être reliées entre elles.

Le traitement s'appuie sur une fonction élémentaire de « Device finger print » que l'on peut traduire par « Empreinte digitale de l'appareil ».

La finalité de cette fonction élémentaire est de signer de manière unique un matériel connecté.

Un script Java de BounceX est chargé sur la page de paiement sur le navigateur du matériel utilisé pour gérer cette transaction de paiement. Ce script collecte des données techniques contextuelles du matériel et les transmet au serveur Privacy Shield Compliant de BounceX.

A partir de ces données, un algorithme propriétaire est joué sur le serveur pour générer un token pour ce matériel. Les données techniques contextuelles du matériel sont IP address, Network session information, Network cache information, Browser identification, URL, User agent. Toutes ces données contextuelles sont collectées et gérées par BounceX.

Payline stocke uniquement le token.

Le token est unique et durable; il permet de signer le terminal à l'origine de la transaction électronique.

- Unique car cette signature ne pourra en aucun cas être générée pour un autre terminal
- Durable car la même signature sera générée pour ce terminal lors d'une transaction ultérieure.

Le token est une donnée chiffrée, non déterministe, ni discriminante qui ne permet en aucun cas d'identifier l'appareil (nature, localisation, propriétaire).

3 Données concernées

3.1.1 Données commerçant

Les catégories de données traitées sont les suivantes :

- données d'identification (nom, prénom, adresse email, identifiant),
- données de connexion : login, mot de passe et adresse IP

3.1.2 Données consommateur

Les données consommateur sont soit transmises à Monext par le Client ou le Moyen de Paiement, soit collectées par Monext pour le compte du Client.

Les catégories de données traitées sont les suivantes :

- données d'identification, (selon les cas : N° de carte bancaire, nom, prénom, adresse de livraison, de facturation, numéros de téléphone, données du moyen de paiement….
- données de localisation,
- dans le cas de l'option « Ubiquité digitale », (identifiants OS, adresse IP)
- autres données (notamment les données « panier » c'est-à-dire la description des achats).

4 Localisation des traitements et des données

Les données sont traitées et stockées en France (Data Centres à Brest, Rennes et Roubaix)

Les données collectées par BounceX sont gérées sur un serveur aux US (Serveur Privacy Shield Compliant de BounceX).

5 Transmission des données à des tiers

5.1 Banques acquéreur

Banques acquéreur avec lesquels le Client possède un contrat commerçant et passerelles techniques avec lesquelles les banques acquéreur sont en contrat.

5.2 Moyens de paiement

Les moyens de paiement acceptés par le Client, avec lesquels le Client est en contrat.

5.3 Sous-traitants

Nom	Domaine	Localisation
ACI	Connexion à certains moyens de paiement et certains acquéreurs	UE
Limonetik	Connexion à certains moyens de paiement et certains acquéreurs	UE
OVH	Hébergement données Back-Office	UE
Zendesk	Gestion Service Clients	UE
Arkéa	Datacentre	UE
Salesforce	Gestion de prospect et contrat	UE

5.4 Co-Responsables de traitement

Nom	Domaine	Localisation
BounceX	Device Finger Printing	US

6 Moyens mis en œuvre pour sécuriser les traitements

Les moyens mis en œuvre pour sécuriser les traitements et les données sont décrits dans l'Annexe « **Sécurité des traitements et des données** ».

7 Droit des personnes (format de transmission des données)

Monext fournit les données demandées par le Client sous forme d'un fichier au format .CSV sous un délai maximum d'un mois, sous réserves des dispositions réglementaires applicables.

La transmission des données de Monext vers le Client s'effectue selon une procédure sécurisée : utilisation des liens existants ou procédure exceptionnelle sécurisée (chiffrement des données, remise en mains propres ou expédition d'un support physique).

Le client effectue sa demande à travers le portail dédié à l'adresse support@payline.com en effectuant une demande typée « Exercice d'un droit RGPD ».

Monext reporte cette demande pour ce qui concerne les données manipulées par BounceX (LCLF : règle d'ubiquité digitale). L'exercice du droit d'accès se fait auprès de BounceX :

https://www.bouncex.com/privacy/data-request-instructions

privacy@bounceexchange.com

8 Portabilité

Monext restitue ses données au Client sous forme d'un fichier au format .CSV

La transmission des données de Monext vers le Client s'effectue selon une procédure sécurisée : utilisation des liens existants ou procédure exceptionnelle sécurisée (chiffrement des données, remise en mains propres ou expédition d'un support physique).