

POLITIQUE DE CONFIDENTIALITÉ RELATIVE À L'UTILISATION DU SERVICE PIX ORGA

V. 26.01.2022

Table des matières

Politique de confidentialité	3
1. Préambule	3
2. Qualifications	3
3. GIP Pix responsable de traitement	3
4. GIP Pix Sous-traitant	4
4.1 Description des traitements	4
4.2 Obligations du Client	4
4.3 Obligations du GIP Pix	5
4.4 Sécurité	6
4.5 Violation de données	7
4.6 Sous-traitance	7
4.7 Flux transfrontières de données	7
4.8 Conservation des données	8
4.9 Audit et vérifications	8
4.10 Coopération	8

Accord de sous-traitance

[En application de l'article 28 du RGPD]

1. Préambule

Le GIP Pix d'une part et le partenaire ou client d'autre part, reconnaissent que l'ensemble des données à caractère personnel auxquels ils auraient accès dans le cadre des services et prestations est soumis au respect de la réglementation applicable en France et dans l'Union européenne dans le domaine de la protection des données à caractère personnel (« réglementation sur la protection des données »), incluant notamment :

- la loi relative à l'informatique, aux fichiers et aux libertés n° 78-17 du 6 janvier 1978 modifiée et ses mises à jour ;
- le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (règlement général sur la protection des données) abrogeant la Directive 95/46/CE (« RGPD »), applicable à partir du 25 mai 2018 ;
- le cas échéant, les textes adoptés au sein de l'Union européenne et les lois locales susceptibles de s'appliquer aux données à caractère personnel traitées dans le cadre de la convention ;
- les textes et décisions émanant d'autorités de contrôle, notamment de la Commission nationale de l'Informatique et des libertés (Cnil) ;
- le cas échéant, les textes, recommandations édictées par le CEPD ou de toute organisation ou autorité dans le secteur de la protection des données à caractère personnel ;
- la réglementation relative à la protection de la vie privée.

2. Qualifications

Dans le cadre de ses rapports avec les utilisateurs et utilisateurs finaux du partenaire ou du client tels que définis au contrat ou aux conditions générales d'utilisation en vigueur entre celui-ci et le GIP Pix, le GIP Pix pourra être respectivement considéré comme responsable de traitement, au titre de la gestion administrative des services (article 3 ci-après) et sous-traitant (article 4 ci-après) au sens de la réglementation susvisée en préambule, au titre de l'utilisation des services (y compris lors de l'activation de l'espace organisation pour le compte du client et de l'hébergement des données).

3. GIP Pix responsable de traitement

Le GIP Pix, en qualité de responsable de traitement dans le cadre de la gestion administrative des services peut être amené à collecter les données à caractère personnel des personnels utilisateurs de Pix Orga suivantes : nom, prénom, adresse électronique du compte Pix associé, indication du rôle d'administrateur Pix Orga et périodes d'exercice du rôle, historique de signature des CGU Pix Orga ; identifiant de connexion, mot de passe.

La collecte desdites données est réalisée pour les besoins internes du GIP Pix en vue de la seule gestion administrative des services objets du présent contrat.

En application de la loi informatique et libertés du 6 janvier 1978 modifiée, l'ensemble des droits des personnes concernées, dont les données sont collectées, traitées et conservées (droit d'accès, droit de rectification, droit d'effacement et droit à la limitation du traitement,, droit à définir le sort de ses

données à cause de décès et droit de ne pas faire l'objet d'une décision individuelle) doivent être exercés par ces personnes auprès du GIP PIX par email à l'adresse dpo@pix.fr.

L'ensemble des informations visées au présent paragraphe est porté à la connaissance des personnels utilisateurs du service Pix Orga par le partenaire ou client et figurent à la politique de confidentialité figurant sur le site pix.fr.

4. GIP Pix Sous-traitant

Le présent paragraphe définit les conditions dans lesquelles le GIP Pix en tant que sous-traitant s'engage à :

- effectuer pour le compte du partenaire ou client les opérations de traitement de données à caractère personnel définies ci-après,
- adopter les mesures techniques et d'organisation liées à la sécurité, en vue de protéger les données à caractère personnel auxquelles il a accès.

4.1 Description des traitements

Le GIP Pix est autorisé à traiter des données à caractère personnel pour le compte du partenaire ou client dans le cadre de l'exécution des services objet du contrat.

Objet & finalités. Le traitement de données à caractère personnel réalisé par le GIP Pix a pour objet et finalité exclusifs l'exécution des services prévus dans le cadre des conditions générales de vente, en ce compris l'activation de l'espace organisation pour le compte du partenaire ou client et l'hébergement des données.

Les traitements mis en oeuvre concernent les finalités suivantes :

- Création de l'espace Pix Orga ;
- Accès à l'espace Pix Orga par le client ou partenaire ;
- Gestion des parcours de tests, suivi des participations, exploitation des résultats par le client ou partenaire.

Nature. Les opérations réalisées sur les données sont les suivantes :

- consultation et utilisation des données, collecte, organisation, structuration, modification, extraction, communication par transmission ;
- conservation, effacement et destruction dans le cadre de l'hébergement et des sauvegardes des données ;
- rapprochement, interconnexion, diffusion technique.

Durée. Par principe, et sauf instruction contraire du partenaire ou client, la durée du traitement réalisée par le GIP Pix est limitée à la durée des conditions générales de vente et du service.

Catégories de personnes concernées. Les données à caractère personnel objet des traitements concernent les catégories suivantes de personnes : les personnes invitées par le partenaire ou client dans le cadre des campagnes de test lancées par lui ou rattachés à son espace Pix Orga et les espaces des structures qui lui sont rattachées le cas échéant.

Type de données. Les données à caractère personnel traitées par le GIP Pix concernent les catégories suivantes de données (les données facultatives sont indiquées entre crochets) :

- Identité : nom(s) et prénom(s), adresse email, identifiants de connexion, et logs de connexion.
- Identifiants : [Identifiant local au client (identifiant interne à l'organisation cliente, par exemple numéro de matricule, adresse électronique professionnelle ou institutionnelle, etc.)]
- Données applicatives : identifiant de campagne, nom de campagne, code parcours, nom du parcours, pourcentage de progression, date de début de parcours, partagé (oui/non), date de partage, détail des acquis validés, détail des acquis évalués et taux de réussite par compétence.

4.2 Obligations du partenaire ou client

Le partenaire ou client s'engage à :

- donner accès au GIP Pix aux données visées au présent document lui permettant de réaliser les opérations visées ci-dessus ;
- documenter par écrit les instructions concernant le traitement des données par le GIP Pix ;
- réaliser les démarches et éventuelles formalités préalables auprès de la Cnil ;
- superviser le traitement.

4.3 Obligations du GIP Pix

Le GIP Pix prend les mesures utiles et/ou nécessaires au respect par lui-même et par son personnel de ses obligations en tant que sous-traitant et notamment à :

- ne pas traiter et consulter les données ou les fichiers à d'autres fins que l'exécution des prestations objet de la présente convention qu'il effectue pour le compte du partenaire ou client au titre du présent document ;
- ne pas traiter, consulter les données en dehors du cadre des instructions documentées et des autorisations reçues du partenaire ou client , y compris en ce qui concerne les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, à moins que le GIP Pix ne soit tenu d'y procéder en vertu d'une disposition impérative résultant du droit communautaire ou du droit de l'Etat membre auquel il est soumis. Dans ce cas, le GIP Pix informe le partenaire ou client de cette obligation juridique avant le traitement des données, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public ;
- informer immédiatement le partenaire ou client si, selon lui, une instruction constitue une violation de la réglementation sur la protection des données.

Les parties conviennent de définir la notion d'instruction comme étant acquise lorsque le GIP Pix agit dans le cadre de l'exécution de la présente convention, ainsi que de toute convention en vigueur entre lui et le partenaire ou client, et notamment les conditions générales de vente applicables qui font référence au présent accord.

Le partenaire ou client reconnaît que la fourniture des prestations pourra impliquer l'établissement d'études et/ou de statistiques afin d'améliorer la qualité des prestations, et plus généralement de la plateforme Pix Orga, et/ou de mesurer les compétences numériques par secteur d'activité et/ou par secteur géographique.

Ainsi, le GIP Pix est susceptible de procéder à l'anonymisation, la pseudonymisation et l'agrégation des données à caractère personnel du partenaire ou client pour permettre au client ou partenaire d'exploiter librement ces données statistiques anonymisées (et les lui mettre à disposition au sein de

tableaux de bord). Le GIP Pix pourra également librement exploiter les données anonymisées pour ses propres besoins et ceux de ses clients et partenaires (statistiques globaux et agrégés, benchmark).

Le GIP Pix s'engage à prendre toute mesure utile afin de garantir que les personnes physiques agissant sous son autorité et ayant accès aux données à caractère personnel ne les traite pas, excepté sur instruction du partenaire ou client, à moins d'y être obligé par une disposition impérative résultant du droit communautaire ou du droit d'un Etat membre de l'Union européenne applicable aux traitements objet de la présente politique de confidentialité.

Le GIP Pix veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité des données ou soient soumises à une obligation légale appropriée de confidentialité.

4.4 Sécurité

Le GIP Pix s'engage avec le partenaire ou client et conformément à la réglementation sur la protection des données, à prendre toutes précautions utiles au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données des fichiers.

Ils mettent en œuvre toutes mesures techniques et organisationnelles appropriées pour protéger les données à caractère personnel, en prenant en compte l'état des connaissances, les coûts de mise en œuvre et la nature, portée, contexte et les finalités du traitement ainsi que les risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, afin de garantir un niveau de sécurité adapté au risque. Ces mesures peuvent comprendre entre autres, selon les besoins :

- le chiffrement des données à caractère personnel ;
- des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
- des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

Les mesures mises en place ou en cours de mise en place par le GIP Pix sont les suivantes :

1) Mesures mises en œuvre sur le plan logique :

- Un contrôle des accès logiques est mis en œuvre, seules les personnes habilitées peuvent accéder aux données et les modifier ;
- Un Identifiant (login) unique est attribué à chaque utilisateur ;
- Des sauvegardes ou synchronisations régulières des données et leur vérification ;
- L'installation dans les meilleurs délais des mises à jour critiques est effectuée ;
- La disponibilité des données est mise en œuvre par des mesures appropriées ;
- Les données sont stockées dans des bases et tables qui sont nativement chiffrées en utilisant un algorithme de chiffrement : Les données sont chiffrées en transit avec TLS et au repos (Encryption at Rest) ;
- Il est vérifié qu'aucun mot de passe ou identifiant ne passe dans les url ;
- Des modalités d'accès spécifiques et restreintes aux données archivées sont mises en œuvre (lorsque les données sont en base d'archivage intermédiaire) ;
- Les archives obsolètes sont détruites de manière sécurisée ;
- Les données sont chiffrées avant leur envoi ;

- Des mesures contre les attaques par injection de code SQL, de scripts, sont mises en œuvre, ainsi que des outils d'analyse et de détection des codes malveillants ;
- Un service de gestion des automates de navigation et Réseau de diffusion de contenu (Content Delivery Network-CDN), visant à identifier les robots de navigation et les comportements malicieux au sein du trafic ;
- Seules les personnes habilitées peuvent toucher au code et le gérer et des revues sont effectuées avant chaque intégration (mise en production) ;
- Des vérifications permettent de s'assurer du bon destinataire des données ;
- L'utilisation des algorithmes, des logiciels et des bibliothèques tiers/tierces reconnues ;
- Le stockage sur des supports de sauvegarde dans un endroit sécurisé de nature à permettre la disponibilité des données, dans un environnement qualifié SecNumCloud ou similaire, pour les données principales ;
- La supervision et le test régulier de la continuité d'activité ;
- L'application des principes de la protection de la vie privée, y compris les exigences de sécurité des données, dès la conception ;
- La traçabilité est mise en œuvre au moyen d'un outil d'enregistrement des logs permettant leur analyse. Les requêtes et les actions sur les comptes sont tracées ;
- L'évolution des tables et des bases de données est faite de façon automatisée via des scripts de migration transactionnel ;
- La sécurité des sites web est assurée aussi par : (i) les communications natives HTTP2 et HTTPS et (ii) la restriction et gestion des accès aux différentes fonctionnalités par un système d'authentification/autorisation basé sur le protocole OAuth2 ;
- Les Tests ont lieu sur des données fictives ou anonymisées.

2°) Mesures mises en œuvre sur le plan physique :

- Contrôle des accès physiques dans les locaux ;
- Verrouillage des postes ;
- Antivirus ou système de protection équivalent ;
- Référencement du parc machine ;
- Reformatages des matériels restitués ;
- Les flux réseau sont limités au strict nécessaire ;
- Le protocole WPA2, WPA2-PSK ou tout nouveau protocole de sécurité apportant un niveau supérieur de sécurité est appliqué pour les réseaux Wi-Fi ;

3°) Mesures mises en œuvre sur le plan organisationnel :

- Politique de sécurité des systèmes d'information (PSSI) ;
- Capitalisation au fur et à mesure de procédures de gestion des demandes des personnes concernées, permettant d'identifier le processus applicable ;
- Registre des incidents comportant un processus formalisé d'analyse et de notification ;
- Contrat assurance cybersécurité comportant une prestation d'assistance ;
- Procédures pour les notifications de violation de données à caractère personnel ;
- Clause spécifique dans les contrats des sous-traitants de rang 2 ;
- Information et sensibilisation des personnes manipulant les données ;
- Limitation de l'accès aux outils et interfaces d'administration aux seules personnes habilitées ;
- Politique spécifique de mots de passe pour les administrateurs ;
- Encadrement par un responsable de l'organisme des interventions par des tiers ;
- Transmission du secret lors d'un envoi distinct et via un canal différent.

4.5 Violation de données

Le GIP Pix s'engage à notifier au partenaire ou client, dans les meilleurs délais après en avoir pris connaissance, toute violation de donnée à caractère personnel, selon les formes légalement requises, soit toute violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

Le GIP Pix s'engage à collaborer activement avec le partenaire ou client pour qu'il soit en mesure de répondre à ses obligations réglementaires et contractuelles. Il revient uniquement au partenaire ou client, en tant que responsable du traitement, de notifier cette violation de données à l'autorité de contrôle compétente ainsi que, le cas échéant, à la personne concernée.

Le client ou partenaire s'engage à communiquer au GIP Pix les coordonnées de la personne à contacter en cas de violation de données (Délégué à la protection des données ou autre représentant). Il appartient au client ou partenaire de transmettre tout changement de ces coordonnées, et de s'assurer de leur exactitude.

4.6 Sous-traitance

Le GIP Pix peut sous-traiter, au sens de la réglementation sur la protection des données, tout ou partie des traitements, notamment vers un pays qui n'est pas situé dans l'Union européenne, en permettant au responsable de traitement, client ou partenaire d'émettre des objections sur information préalable, sauf si ce changement est nécessaire à la continuité, à la sécurité ou la mobilisation de ressources humaines pour des services fournis par le GIP Pix, ou résulte d'un marché régulièrement soumis au code de la commande publique. L'objection est formulée dans un délai raisonnable n'excédant pas quinze (15) jours calendaires par écrit auprès du GIP Pix et précise un motif raisonnable et légitime. Dans l'hypothèse où une objection a été émise, les parties se rapprocheront pour discuter de bonne foi des modalités raisonnables et appropriées de la poursuite des traitements où à défaut, de leur terme.

Le client accorde, par les présentes, une autorisation générale de sous-traitance conformément à l'article 28 du Règlement UE 2016/479.

Le GIP met à la charge de son sous-traitant ultérieur toutes obligations nécessaires pour que soient respectées la confidentialité, la sécurité et l'intégrité des données, et pour que lesdites données ne puissent être ni cédées ou louées à un tiers à titre gratuit ou non, ni utilisées à d'autres fins que celles définies dans le présent document.

La liste des sous-traitants du GIP Pix figure à cette adresse : [Lien vers la liste des sous-traitants](#).

4.7 Flux transfrontières de données

En cas de transfert de données à caractère personnel vers un pays tiers n'appartenant pas à l'Union européenne, ou vers une organisation internationale, le GIP Pix en informe le partenaire ou client et s'engage à coopérer avec lui afin d'assurer :

- le respect des procédures permettant de se conformer à la réglementation Informatique et libertés, par exemple dans le cas où une autorisation de la part de la Cnil apparaîtrait nécessaire ;

- si besoin, la conclusion d'un ou plusieurs contrats permettant d'encadrer les flux transfrontières de données. Le GIP Pix s'engage en particulier, si nécessaire, à signer de tels contrats avec le partenaire ou client et/ou à obtenir la conclusion de tels contrats par ses sous-traitants. Dans la mesure où le partenaire ou client est situé dans un pays tiers à l'Union européenne qui n'est pas reconnu comme présentant un niveau de protection équivalent à la réglementation européenne, il est convenu entre les parties que les clauses contractuelles types publiées par la Commission européenne sont utilisées pour encadrer les flux transfrontières de données. Elles sont accessibles et téléchargeables au lien suivant : <https://cloud.pix.fr/s/2pr5pykTXa9psp5>.

L'accord du partenaire ou client est acquis concernant certaines données susceptibles de faire l'objet d'un transfert vers l'Union européenne par les sous-traitants Datadog (sécurité) uniquement pour fournir un service de support, SendInBlue (envoi de courriers électroniques) et Freshworks (service support), uniquement pour permettre la maintenance du service (24/24h) et suivre le compte du GIP Pix.

Ces transferts sont effectués conformément à la réglementation en vigueur concernant la protection des données à caractère personnel :

- un contrat spécifique a été conclu avec ces sous-traitants permettant de s'assurer qu'il présentent des garanties appropriées concernant la protection des données, et contenant les clauses contractuelles types de la commission européenne ;
- ces sous-traitants ont justifié mettre en œuvre les mesures supplémentaires permettant d'assurer aux données faisant l'objet d'un transfert un niveau de protection essentiellement équivalent à celui de l'Union européenne conformément à l'arrêt de la Cour de Justice de l'Union européenne dit Schrems II.

4.8 Conservation des données

Au terme de la convention, et sauf disposition impérative contraire résultant du droit communautaire ou du droit d'un Etat membre de l'Union européenne applicable aux traitements objets de la présente politique de confidentialité, le GIP Pix s'engage, au choix du partenaire ou du client, soit à détruire tous fichiers manuels ou informatisés stockant les informations collectées en exécution des accord avec le partenaire ou client, soit à renvoyer l'intégralité des données à caractère personnel au client ou à tout sous-traitant désigné par le client.

Le partenaire ou client est informé et accepte qu'au terme de la convention en vigueur entre lui et le GIP Pix, le GIP Pix conserve les données à caractère personnel pour une durée complémentaire de trois (3) mois à compter du terme de la convention. Celle-ci continue à produire ses effets pour les seuls besoin de la conservation de ces données au bénéfice du partenaire ou client et lui permettre de les récupérer s'il le souhaite pendant cette durée en les exportant au moyen des services (export .csv).

Le partenaire ou client est informé et accepte que les données à caractère personnel de nature applicative de l'utilisateur final des services, ayant rejoint une campagne et réalisé un ou plusieurs parcours, restent accessibles par cet utilisateur lequel peut continuer à consulter les résultats de ces campagnes.

4.9 Audit et vérifications

A la demande du client, le GIP Pix devra établir une attestation ou transmettre toute information utile pour démontrer que les règles prévues par le présent document, et de manière générale ses obligations en matière de données à caractère personnel ont bien été respectées.

Le client se réserve le droit de procéder à des inspections et audits qui lui paraissent utiles pour constater le respect des obligations précitées, et notamment en procédant à un audit de sécurité auprès du GIP Pix, y compris en ayant recours à un tiers soumis à un engagement approprié de confidentialité qui n'est pas un concurrent direct ou indirect du GIP Pix.

Le client et le GIP Pix définiront au sein d'un accord distinct, le périmètre et le calendrier de l'audit, les mesures de sécurité et de confidentialité appropriées, préalablement à son déroulement, ainsi que les modalités éventuelles de partage des frais. Sauf accord contraire, les frais d'audit restent à la charge du client.

4.10 Coopération

Le GIP Pix s'engage à coopérer avec le client afin de permettre :

- la gestion des demandes des personnes concernées par les traitements tendant à l'exercice de leurs droits. Si une personne concernée devait contacter directement le GIP Pix pour exercer ses droits d'accès, de rectification, de suppression et/ou d'opposition ou pour toute autre demande liée à la protection des données à caractère personnel, le GIP Pix communiquera au client dans un délai raisonnable les demandes qui lui seront parvenues. Le GIP Pix ne pourra répondre à la demande d'une personne concernée que sur instruction du client ;
- la réalisation de toute analyse d'impact que le client déciderait d'effectuer, afin d'évaluer les risques qu'un traitement fait peser sur les droits et libertés des personnes et d'identifier les mesures à mettre en œuvre pour faire face à ces risques, et la consultation de l'autorité de contrôle ;
- plus généralement, le respect des obligations pesant sur le client au regard de la réglementation sur la protection des données, telles que notamment ses obligations de notification à l'autorité de contrôle et de communication d'une violation de données aux personnes concernées.

La coopération du GIP Pix ne fait pas l'objet de frais dans la mesure où elle lui est demandée dans des proportions raisonnables et n'excède pas ce qui est strictement nécessaire pour la fourniture des services conformément à la réglementation.

En cas de contrôle d'une autorité compétente, les parties s'engagent à coopérer entre elles et avec l'autorité de contrôle.

En cas de contrôle d'une autorité compétente chez le client portant notamment sur les services délivrés par le GIP Pix, ce dernier s'engage à coopérer avec le client et à lui fournir toute information dont le client pourrait avoir besoin ou qui s'avérerait nécessaire.