CONDITIONS GENERALES UTILISATEUR
*
FNC-RF
FICHIER NATIONAL DES COMPTES BANCAIRES SIGNALES POUR RISQUES DE FRAUDE

Table des matières

LISTE DES ANNEXES

Préambule

Afin de renforcer les outils de lutte contre la fraude aux paiements à disposition des Prestataires de services de paiement (PSP), le fichier national des comptes bancaires signalés pour risque de fraude (FNC-RF), dédié au partage d'informations relatives aux comptes identifiés comme étant associés à des transactions pour lesquelles des suspicions de fraude existent ou des fraudes sont avérées, vise à renforcer le taux de détection des tentatives de fraude au virement chez l'ensemble des PSP.

Ce dispositif est mis en œuvre conformément à l'article L.521-6-1 du Code monétaire et financier et aux arrêtés pris pour son application. La Banque de France en assure la gouvernance et la réalisation, avec la collaboration de l'ensemble des parties prenantes.

Le choix de la solution technique retenue pour implémenter la Plateforme de partage s'est porté sur le logiciel MISP[1], dont le principe de fonctionnement est adapté au contexte de la lutte contre la fraude aux moyens de paiement, comme en atteste son utilisation par l'European Payments Council (EPC) ainsi que par plusieurs pays européens.

Le périmètre des données partagées au sein du FNC-RF est susceptible d'évoluer avec le temps, ce qui impliquerait le cas échéant de devoir amender en conséquence les présentes conditions générales d'utilisation (CGU) qui seront notifiées aux utilisateurs dans les formes prévues.

Article 1. Objet des conditions générales

Les présentes CGU ont pour objet de préciser les conditions de participation et d'utilisation du FNC-RF

L'article L 521-6-1 du Code Monétaire et Financier ainsi que l'arrêté mentionné au VI du même article définissent le cadre juridique de ce partage d'informations. Les présentes CGU se fondent sur les dispositions prévues dans cet article de loi qui prévaut sur toute autre considération en matière de règles encadrant le dispositif FNC-RF.

À la date d'entrée en vigueur des présentes CGU, la Banque de France, en qualité de tiers de confiance, est Administrateur du FNC-RF en vertu de l'article de L.521-6-1 du Code Monétaire et Financier. À ce titre, elle assure le fonctionnement du dispositif et veille au respect de l'ensemble des obligations mises à la charge des utilisateurs dans les présentes CGU et par la réglementation applicable.

Article 2. Définitions et abréviations

Au sens des présentes CGU, on entend par :

FNC-RF : Plateforme de partage des données de fraude et de suspicion de fraude se fondant sur la solution technique MISP, hébergée et gérée par l'Administrateur. Elle est mise en œuvre dans le cadre des dispositions prévues par l'article L 521-6-1 du code monétaire et financier.

AC : autorité de certification reconnue par la Banque de France.

Administrateur : personne morale qui gère le FNC-RF, préside et organise le Comité de Pilotage. Ce rôle est occupé par la Banque de France, tel que précisé dans l'article L 521-6-1 du code monétaire et financier.

Anomalie : Une anomalie est un écart constaté entre le fonctionnent attendu d'un système informatique et son fonctionnement réel.
Elle révèle qu'un composant—logiciel, matériel, donnée, processus ou documentation—ne fonctionne pas conformément aux spécifications, aux besoins métiers ou aux normes de qualité définies dans le projet.
Une anomalie peut notamment correspondre à :

[1] MISP est aujourd'hui adopté par de nombreux CERT, CSIRT et SOC, que ce soit pour des projets de partage d'informations au sein d'une communauté, ou en interne pour gérer des indicateurs de compromission.

- Un dysfonctionnement : une fonctionnalité ne fonctionne pas ou fonctionne de manière incorrecte.
- Une incohérence : un résultat fourni par le système diffère du résultat attendu.
- Une non-conformité : un écart par rapport aux spécifications fonctionnelles, techniques ou aux exigences réglementaires.
- Un défaut de performance : lenteur, surcharge, mauvaise optimisation.
- Un comportement imprévu : erreur, crash, blocage, messages incohérents.

API : ***Application Programming Interface,*** interface standardisée mise à disposition par la Plateforme FNC-RF dans le cadre des échanges de données avec les Participants n'ayant pas choisi d'utiliser le mode de synchronisation avec le MISP central géré par l'Administrateur.

Certificat électronique : désigne les certificats d'authentification permettant de se connecter au FNC-RF.

Chef de file : le Participant qui accède à la Plateforme FNC-RF pour le compte des autres Participants faisant partie du même groupe.

Clé d'authentification MISP : clé générée par l'Administrateur sur l'Utilisateur de synchronisation MISP. Elle est nécessaire pour autoriser l'accès au FNC-RF et garantir la traçabilité des connexions.

Comité de Pilotage : instance de gouvernance du FNC-RF, présidée par l'Administrateur, qui pilote l'administration de la Plateforme, la gestion des accès, la gestion des Incidents, ainsi que des évolutions et tout autre sujet relatif au FNC-RF.

Détenteur de compte : Participant teneur d'un compte associé à un Évènement de fraude déclaré dans le FNC-RF.

Évènement de fraude : ensemble d'informations relatives à une suspicion de fraude ou à une fraude, partagé au sein de la Plateforme FNC-RF et dont l'Identifiant de compte est l'élément central.

Identifiant de compte : numéro identifiant de manière unique un compte bancaire, pouvant prendre la forme d'un IBAN (normalisation au niveau international, obligatoire dans les opérations de paiements SEPA), ou BBAN pour certains comptes domiciliés dans des pays se situant en dehors de la zone SEPA**.** Cet identifiant est utilisé comme référence unique dans le cadre des déclarations au FNC-RF.

Incident : tout dysfonctionnement complet ou partiel survenant en production, qui ne fait pas partie du fonctionnement standard de la Plateforme FNC-RF, et se traduisant par une diminution de la qualité de service offert par le FNC-RF.

KPI : ***Key Performance Indicator***, indicateur chiffré visant à mesurer l'efficacité du FNC-RF ainsi que le respect de ses règles de fonctionnement, dans une optique d'amélioration continue du dispositif.

Mandataire de Certification (MC) : désigne une personne physique habilitée par le représentant légal du Participant à demander à l'autorité de certification de la Banque de France la création ou la révocation de certificats d'authentification.

MISP : ***Malware Information Sharing Platform*** est un logiciel open source de renseignement sur les menaces, adapté au contexte de la fraude aux moyens de paiement dans le cadre de la mise en œuvre du FNC-RF.

Participant : ensemble des Participants actifs ou en consultation.

Participant actif : prestataire de service de paiement accédant au dispositif FNC-RF et disposant de droits lui permettant de consulter et d'alimenter le FNC-RF.

Participant en consultation : personne morale ayant accès au dispositif FNC-RF en lecture seule, sans possibilité de modifier ou d'alimenter les données.

Partie : Tout Participant acceptant ces CGU, ainsi que l'Administrateur.

Plateforme : service de communication en ligne permettant le partage de données entre les Participants, mis à disposition par l'Administrateur.

Prestataire technique: Société de services informatiques mandaté par un Participant comme intermédiaire pour accéder à la Plateforme FNC-RF. Ce prestataire ne possède pas nécessairement un agrément de prestataire de service de paiement, et peut être interne ou externe à l'organisation du PSP mandant.

PSP: Prestataire de services de paiement tels que mentionnés à l'article L. 521-6-1 du code monétaire et financier.

Qualification Détenteur de Compte : évaluation du caractère potentiellement frauduleux d'un compte faisant l'objet d'une déclaration dans le FNC-RF qui est réalisée par le Participant détenteur du compte.

Qualification Participant : complément d'évaluation réalisée par tout Participant sur la base des informations à sa disposition.

Système local : terme désignant les systèmes mis en œuvre par les Participants pour stocker, transmettre ou récupérer les données centralisées par le FNC-RF.

Spécifications Externes Générales : document listant les règles de gestion régissant le fonctionnement de la Plateforme FNC-RF.

Utilisateur de synchronisation : utilisateur dédié à un Participant géré en central par l'Administrateur disposant des rôles nécessaires pour autoriser les échanges de flux.

Article 3. Documents contractuels

La participation au FNC-RF est régie par les présentes CGU, ainsi que les documents associés, à savoir :

Les bulletins et formulaires :

- **Le bulletin d'adhésion et de renseignement :** ce document intègre l'ensemble des informations relatives au Participant. Par la signature de ce bulletin, le Participant exprime son accord et acceptation des présentes CGU.
- **Le formulaire de raccordement** : ce document intègre l'ensemble des informations techniques et organisationnelles relatives à son mode de raccordement au FNC-RF.
- **Le formulaire de mise à jour du référentiel de BIC :** document transmis par le Participant permettant de renseigner le référentiel de BIC (Bank Identifier Code) géré par l'Administrateur.
- **Le bulletin de facturation** : ce document intègre l'ensemble des éléments relatifs aux modalités tarifaires ainsi que les informations nécessaires à l'exécution des paiements réalisés par le participant au titre de sa participation au FNC-RF.

La documentation technique précisant les modalités techniques de raccordement, d'échange et de sécurité annexée au présentes CGU :

- Les Spécifications Externes Générales.
- Les Spécifications Externes Détaillées.
- La documentation complémentaire

Les documents annexés aux présentes CGU en font partie intégrante et sont considérés comme formant un tout indivisible. En cas de contradiction, les présentes CGU prévalent sur tout autre document à l'exception des dispositions législatives et règlementaires en vigueur.

Article 4. Demande d'accès au FNC-RF

4.1. Dispositions générales

Les Prestataires de services de paiement (PSP) disposant d'un statut leur permettant de participer au FNC-RF sont définis dans l'article L 521-6-1 du code monétaire et financier.

Le PSP souhaitant devenir Participant adresse à l'Administrateur l'ensemble des bulletins et formulaires cités à l'article 3 dûment complétés et signés en respectant le délai de préavis fixé par le Comité de Pilotage du FNC-RF avant la date effective de prise d'effet de l'adhésion.

La réception et l'acceptation de ces bulletins et formulaires par l'Administrateur conditionnent l'accès effectif à la Plateforme.

En cas de modification des informations y figurant, le Participant adresse à l'Administrateur le bulletin ou le formulaire faisant l'objet d'une modification, en respectant, avant la date de prise d'effet souhaitée desdites modifications, le(s) délai(s) de préavis fixé(s) par le Comité de Pilotage.

Ce bulletin ou ce formulaire sont communiqués à l'Administrateur conformément aux dispositions de l'article 15.

4.2. Cas des groupes

L'adhésion au FNC-RF peut se faire pour l'ensemble d'un groupe, par l'entité de son choix, sous réserve qu'elle respecte les conditions relatives à la définition d'un Participant actif, décrites à l'Article 2.

Un groupe peut être constitué d'un Participant actif, appelé "Chef de file" qui accède au fichier pour les établissements rattachés qui mandatent le Chef de file à cet effet, c'est-à-dire :

- pour les entités dont il détient directement ou indirectement la majorité du capital au sens de l'article L.233-1 du Code de commerce, les sociétés et groupements dans lesquels l'une quelconque des sociétés susvisées détiennent, ensemble ou séparément, une participation au sens de l'article L.233-2 du Code de commerce, les sociétés et groupements que l'une quelconque des sociétés susvisées contrôlent, directement ou indirectement, ensemble ou séparément, au sens des articles L.233-3 et L.233-16 du Code de commerce, et les sociétés et groupements sur lesquels l'une quelconque des sociétés susvisées exercent, ensemble ou séparément, une influence dominante au sens de l'article L.233-16 du Code de commerce et/ou une influence notable au sens de l'article L.233-17-2 du Code de commerce ;

- pour un ensemble d'entités affiliées comme lui à un même organe central[2], au sens des articles L. 511-30 et L. 511-31 du Code monétaire et financier – ensembles pouvant notamment être constitués d'entités bénéficiant d'un agrément collectif accordé, en application de l'article R. 511-3 du Code monétaire et financier, à une caisse régionale ou fédérale pour elle-même et pour les caisses locales qui lui sont affiliées ou qui sont affiliées comme elle à une même fédération régionale –, ainsi que pour des entités sur lesquelles une de ces entités affiliées exerce un contrôle exclusif;

- en sa qualité d'organe central, au sens des articles L. 511-30 et L. 511-31 du code monétaire et financier, pour le compte des établissements de crédit qui lui sont affiliés ainsi que des entités sur lesquelles l'un de ses affiliés exerce un contrôle exclusif.

Un établissement ne peut être rattaché qu'à un seul groupe.

Le cas échéant, l'entité Chef de file doit indiquer dans le bulletin d'adhésion les autres entités du groupe pour lesquelles elle agit en mentionnant le code interbancaire (CIB) de ces établissements ; ces dernières devant satisfaire les conditions relatives à la définition d'un Participant actif, décrites à l'Article 2.

Le Chef de file signe le bulletin d'adhésion et de renseignement, le formulaire de mise à jour du référentiel BIC, le bulletin de facturation et le formulaire de raccordement pour l'ensemble du groupe qu'il représente.

L'entité raccordée techniquement à la Plateforme FNC-RF pour le compte de son groupe peut en outre être différente de l'entité chef de file. Dans ce cadre, l'entité raccordée signe elle-même le bulletin de raccordement pour le compte du groupe.

Le Chef de file devient l'unique interlocuteur de l'Administrateur et est responsable de la diffusion des informations qu'il reçoit à l'ensemble des Participants qu'il représente. Toute communication adressée au Chef de file est opposable à l'ensemble des Participants représentés. Si le raccordement est réalisé par une entité distincte, cette dernière pourra recevoir des informations relatives au raccordement directement de la part de l'Administrateur.

Le bulletin d'adhésion fait l'objet d'une actualisation dans l'hypothèse d'une modification portant sur la liste des établissements représentés. Il doit être adressé à l'Administrateur au plus tard un mois avant la date effective de la modification. Le bulletin ainsi mis à jour se substitue à toute version antérieure de celui-ci.

[2] Sous réserve d'être mandaté à l'effet de les représenter

L'Administrateur, dans le cadre de contrôles périodiques et aléatoires, se réserve la possibilité de demander l'envoi d'un nouveau bulletin d'adhésion, y compris en l'absence de modification, afin de s'assurer disposer d'une information à jour.

4.3. Cas des Participants en consultation

L'ensemble des dispositions des présentes CGU s'applique aux entités autorisées à accéder aux données contenues dans le FNC-RF avec le rôle de Participant en consultation, à l'exception de celles demandant au participant d'effectuer une potentielle action conduisant à modifier ces données.

Les Participants en consultation disposent uniquement d'un droit d'accès en lecture et ne bénéficient à ce titre d'aucun droit d'ajout, de modification et de suppression des données contenues dans le FNC-RF.

Article 5. Accès au FNC-RF

5.1. Autorisation d'accès au FNC-RF

Seuls les établissements définis à l'article L. 521-6-1 du code monétaire et financier et dans l'arrêté XX sont habilités à formuler une demande d'accès au statut de Participant.

Le Participant, lorsqu'il formule sa demande d'accès, précise s'il s'agit d'une demande en qualité de Participant actif ou bien de Participant en consultation.

Dans les deux cas, les diligences administratives, techniques et organisationnelles nécessaires à la demande de participation sont entièrement à la charge l'établissement demandeur.

L'Administrateur est seul habilité à donner accès techniquement aux Participants de la Plateforme lorsque ces derniers en formulent la demande et satisfont les conditions prévues à l'article L. 521-6-1 du code monétaire et financier et dans l'arrêté mentionné au VI du L 521-6-1 du code monétaire et financier.

À ce titre, l'accès à la Plateforme de Production est soumis à l'approbation de l'Administrateur, après une phase obligatoire d'homologation sur un environnement informatique de test dédié. L'Administrateur se réserve le droit de refuser ou de différer l'accès en cas de non-conformité ou d'insuffisance des diligences réalisées par le Participant.

5.2. Modes de raccordement

L'interfaçage technique entre le Participant et l'Administrateur peut se faire selon l'une des trois manières suivantes :

- **Synchronisé** : synchronisation entre l'instance MISP du Participant et celle de l'Administrateur ;
- **API :** utilisation d'une interface applicative (API) sécurisée et mise à disposition par l'Administrateur ;
- **Intermédié :** accès via un Prestataire technique assurant le rôle d'intermédiaire, qui pourra lui-même se connecter via une synchronisation avec l'instance de l'Administrateur, ou bien une API.

Dans chaque cas, les Participants auront la charge de mettre en place les interfaces permettant de communiquer avec le FNC-RF et les traitements intermédiaires permettant l'exploitation des données récupérées. Ils demeurent seuls responsables de la conformité, de la sécurité et de la fiabilité des systèmes locaux utilisés pour ces échanges.

5.3. Conditions techniques d'accès

5.3.1. Droits d'accès et authentification

L'accès à la Plateforme de partage nécessite l'authentification de l'Utilisateur de synchronisation rattaché à l'organisation du Participant déclarée dans le FNC-RF via une Clé d'authentification MISP et un certificat Client aux normes du RSI de la Banque de France.

Les certificats numériques utilisés doivent être émis par une Autorité de Certification (AC) reconnue de confiance à la Banque de France (et expressément autorisée par la Banque de France : la liste des AC autorisées est disponible sur l'extranet dédié):

1. Les Autorités de Certification de la Banque de France ;

2. Les Autorités de Certification délivrant des certificats aux normes RGS **/*** ;

3. Les AC qualifiées au sens du règlement eIDAS (electronic Identification, Authentication and Trust Services) et publiées dans la « trusted list » de la commission européenne.

> Dans le cadre du projet de Partage des données de fraude entre PSP, il est recommandé d'utiliser un certificat d'authentification émis par une Autorité de Certification qualifiée RGS**/***. Toutefois, il est autorisé d'utiliser un certificat d'authentification logiciel en respectant la sécurisation du stockage dudit certificat (clé privée).

En cas de raccordement synchronisé, le Participant doit créer un serveur de synchronisation avec la clé communiquée par l'Administrateur et lui associer le certificat client.

En cas de raccordement par mode API, le Participant doit utiliser les *credentials (Client Id et Client secret)* communiqués par l'Administrateur et le certificat client afin de récupérer un Token pour autoriser l'accès. La partie publique du certificat client doit être communiquée au préalable à l'Administrateur pour déclaration dans la base des utilisateurs externes.

Sauf demande expresse de l'Administrateur, le Participant ne doit pas renseigner la date de fin de validité de la Clé d'authentification MISP.

Un seul compte utilisateur est nécessaire par Participant pour les échanges de flux. Cet utilisateur, qui existe uniquement dans le MISP central du FNC-RF, porte les rôles MISP strictement nécessaires au bon déroulement des échanges de flux entre la Plateforme et le Participant.

En cas de nécessité, le Participant peut adresser à l'Administrateur une demande afin que ce dernier génère une nouvelle Clé d'authentification qui sera communiquée au Participant concerné.

L'accès ne sera autorisé qu'aux appareils disposant d'une adresse IP déclarée préalablement par le Participant dans son formulaire de raccordement. Le Participant s'engage à maintenir cette information à jour et à informer l'Administrateur sans délai de toute modification. L'Administrateur ne saurait être tenu responsable des indisponibilités ou Incidents résultant d'une déclaration inexacte ou tardive.

En cas de compromission, ou de suspicion de compromission d'un Certificat électronique, le Participant s'engage à procéder sans délai à la révocation du Certificat électronique auprès de l'autorité qui l'a émis ainsi qu'à en informer immédiatement l'Administrateur qui, sur demande, peut procéder à la désactivation de l'Utilisateur de synchronisation.

5.4. Vérifications préalables au raccordement

5.4.1. Spécificités des Web services du mode API

Les Web services ouverts dans le cadre de la connexion **en mode API** sont décrits dans les Spécifications Externes Détaillées. Tout autre Web service est exclu du fichier de définition dans la brique API FNC-RF et ne sera donc pas accepté.

5.4.2. Homologation

La phase d'homologation client est obligatoire en amont du premier raccordement à la Plateforme centrale FNC-RF en Production. Un procès-verbal de test, dûment signé par le Participant, doit être communiqué à l'Administrateur dans un délai fixé par ce dernier après avis du Comité de pilotage, avant le démarrage des actions de raccordement technique en production.

L'Administrateur refuse l'accès en production en cas de non-conformité ou de défaut de transmission du procès-verbal.

5.4.3. Fonctionnalités du FNC-RF

Les fonctionnalités offertes par le FNC-RF sont précisées dans les documents suivants :

- Les Spécifications Externes Générales (SEG).
- Les Spécifications Externes Détaillées (SED).

5.4.4. Exigences fonctionnelles

L'Administrateur procède à l'intégration automatique dans la Plateforme centrale du FNC-RF les données transmises par les Participants actifs à travers les canaux prévus dans les modes de raccordements décrits dans cet Article. L'intégration de ces données est réalisée selon le modèle de données et les règles décrits dans les Spécifications Externes Générales (SEG).

Avant intégration des données, l'Administrateur doit effectuer les contrôles systématiques de structure prévus au sein des SEG et validées par le Comité de pilotage.

L'Administrateur est tenu de mettre à disposition les données stockées dans le FNC-RF à travers les canaux prévus dans les modes de raccordements décrits dans cet Article.

L'Administrateur est tenu de mettre à jour le référentiel listant les identifiants BIC associés à chacun des Participants actifs Détenteurs de compte, sur la base des informations transmises par ces derniers. Ces mises à jour se font dans les meilleurs délais ou à une date fixée en commun accord avec le Participant demandeur.

En revanche, l'Administrateur :

- n'est pas tenu de se prononcer sur la pertinence des Évènements de fraude déclarés ou sur le caractère frauduleux des identifiants de compte bancaire associés à ces évènements ;
- ne doit pas modifier les données transmises par les établissements, sauf dans les cas prévus au sein des SEG.

5.4.5. Sécurité

D'une manière générale, l'Administrateur s'engage, au terme d'une obligation de moyen renforcée, à mettre en œuvre toutes les mesures de sécurité raisonnables susceptibles de permettre la prévention des intrusions sur le FNC-RF et des atteintes à la confidentialité, à l'intégrité et à la disponibilité du FNC-RF qui surviendraient via son système d'information, y compris ses accès internet.

Le caractère raisonnable desdites mesures s'apprécie notamment sur la base de l'état de l'art en la matière au moment de leur mise en place, ainsi que du coût et de la complexité engendrée par celle-ci au regard de la nature et de l'ampleur des risques encourus. En conséquence, l'Administrateur ne pourra s'exonérer de son éventuelle responsabilité qu'en apportant aux Participants la preuve positive de son absence de faute.

5.4.6. Sauvegarde des données

L'Administrateur s'engage à effectuer une sauvegarde quotidienne des données stockées dans le FNC-RF, avec une rétention maximale de sept jours (J-7).

5.5. Obligations du Participant

5.5.1. Exigences fonctionnelles

Le Participant est tenu d'appliquer l'ensemble des règles spécifiées dans les Spécifications Externes Générales, Spécifications Externes Détaillées, ainsi que l'ensemble des règles d'usage qui seront validées par le Comité de Pilotage. Les Participants sont informés de ces règles par mise à disposition sur le site extranet dédié, le cas échéant par l'intermédiaire de leur Chef de file.

Le Participant actif ne peut effectuer d'échanges de données avec la Plateforme du FNC-RF qu'à travers les canaux prévus dans les modes de raccordements décrits dans l'article 5.2.

Le Participant actif doit, de sa propre initiative, et selon les modalités précisées dans les SEG et SED :

- transmettre vers la Plateforme du FNC-RF les nouvelles données ou modifications de données stockées dans son système local;
- récupérer et intégrer dans son Système local les données stockées dans la Plateforme du FNC-RF.

Il est attendu que cette action de synchronisation entre le Système local du Participant actif et la Plateforme du FNC-RF se fasse selon la fréquence définie dans l'arrêté mentionné à l'article L. 521-6-1 du code monétaire et financier.

L'usage de ces données par le Participant dans le cadre de ses propres traitements de lutte contre la fraude se fait dans les limites prévues par L.521-6-1 du code monétaire et financier.

Le Participant actif est responsable de la qualité, de l'exactitude et de la pertinence des données transmises. Alors même que l'Administrateur met en place les contrôles demandés et spécifiés dans la SEG et SED, il ne peut garantir que les données intégrées dans le FNC-RF soient exemptes de défauts, d'erreurs ou d'omissions.

Il est attendu que le Participant actif applique les règles de suppression des évènements de fraude dans son Système local à l'image de celles appliquées au sein du FNC-RF, précisées dans les Spécifications Externes Générales, et sur la base des délais suivants :

- Purge réglementaire lorsque la durée de rétention atteint la limite définie au sein de l'arrêté mentionné au VI du L.521-6-1 du code monétaire et financier ;
- Suppression des Évènements de fraude identifiés comme tels par le Participant actif les ayant lui-même déclarés.

5.5.2. Sécurité

D'une manière générale, le Participant met en œuvre, au terme d'une obligation de moyen renforcée, toutes les mesures de sécurité raisonnables susceptibles de permettre la prévention des intrusions sur le FNC-RF et des atteintes à la confidentialité, à l'intégrité et à la disponibilité du FNC-RF qui surviendraient via son système d'information, y compris ses accès internet.

Le caractère raisonnable desdites mesures s'apprécie notamment sur la base de l'état de l'art en la matière au moment de leur mise en place, ainsi que du coût et de la complexité engendrée par celle-ci au regard de la nature et de l'ampleur des risques encourus. En conséquence, le Participant ne pourra s'exonérer de son éventuelle responsabilité qu'en apportant à l'Administrateur la preuve positive de son absence de faute.

Le Participant est le seul responsable de la protection appropriée de la confidentialité, de l'intégrité et de la disponibilité de son accès à la Plateforme FNC-RF. Chaque Participant s'engage à informer l'Administrateur, dès qu'il en a connaissance, de tout Incident ou Anomalie lié à la sécurité susceptible d'affecter l'exécution des présentes. Les modalités de gestion des Incidents et des Anomalies sont décrites en Annexe 1.

5.5.3. Systèmes locaux

Comme indiqué dans l'article L 521-6-1 du code monétaire et financier, le Participant est entièrement responsable de la gestion des données issues de la Plateforme du FNC-RF qu'il est amené à traiter dans ses systèmes applicatifs locaux, qu'il s'agisse de copies intégrales ou partielles des données émanant du FNC-RF. Cette responsabilité couvre la conservation, la sécurisation, la suppression et l'utilisation desdites données.

Article 6. Accès aux données dans le cas d'un groupe

Le Participant actif bénéficie de plein droit d'une mise à disposition des données, par l'Administrateur, des données du FNC-RF pour lui-même ainsi que, le cas échéant, pour les entités appartenant à son groupe, sous réserve qu'elles satisfassent les conditions prévues par l'article L 521-6-1 du code monétaire et financier.

Article 7. Accès au FNC-RF par l'intermédiaire d'un Prestataire technique

Le Participant actif est autorisé à faire appel, en tant que de besoin, à un Prestataire technique qui effectuera, en son nom et pour son compte, les échanges de données avec la Plateforme du FNC-RF. Bien qu'il délègue à son fournisseur de services une partie des opérations, le Participant actif assume l'entière responsabilité du respect des présentes CGU et reste l'interlocuteur principal vis-à-vis de l'Administrateur.

Le Participant actif devra notamment s'assurer que le Prestataire technique désigné :

- applique des mesures de sécurité et de protection des données au moins équivalentes à celles attendues d'un Participant, conformément aux SEG et SED ;
- n'exploite pas, ne conserve pas et ne réutilise pas les données qu'il stocke pour le compte du Participant, au-delà du strict nécessaire aux échanges entre le Participant et la Plateforme FNC-RF ;
- respecte l'ensemble des obligations légales et réglementaires applicables en matière de protection des données, notamment le règlement (UE) 2016/679 (RGPD) et la loi Informatique et Libertés ;
- se soumet à toute demande de contrôle ou d'audit diligentée par le Participant ou par l'Administrateur, afin de vérifier la conformité des opérations réalisées.

Lorsque le Participant actif confie l'exploitation informatique à un prestataire technique, celui-ci, en qualité de sous-traitant, est tenu à des obligations similaires à celles du responsable de traitement en application du Règlement (UE) 2016/679 susvisé. Il appartient au Participant actif de s'assurer que son sous-traitant respecte les obligations de la présente convention et présente les mêmes garanties quant à la mise en œuvre des mesures techniques et organisationnelles prévues afin que le traitement réponde aux exigences du Règlement (UE) 2016/679 susvisé. Si le sous-traitant ne remplit pas ses obligations en matière de protection des données, le Participant demeure pleinement responsable devant le responsable de traitement de l'exécution de ses obligations.

Si le Participant actif fait appel à un prestataire technique situé hors de l'Union européenne, il doit préalablement vérifier que ce dernier assure un niveau de protection des données suffisant et approprié. À cet effet, le Participant actif recourt à une décision d'adéquation telle que définie à l'article 45 du RGPD. Le Participant actif inclut dans ses contrats avec les sous-traitants, en application des articles 46 et 47 du RGPD, les clauses contractuelles types publiées par la Commission Européenne, exécutoires en l'absence d'autres garanties complémentaires susvisées.

Article 8. Gouvernance du FNC-RF

8.1. Comité de Pilotage

Un Comité de Pilotage associant l'ensemble des Participants et les associations représentatives de ces derniers, se réunit périodiquement afin d'examiner notamment les conditions de fonctionnement du FNC-RF, l'efficacité de la Plateforme, les Demandes d'évolutions des Participants, ainsi que toute question relative à la sécurité et à la conformité réglementaire de la Plateforme.

L'Administrateur est membre de droit de ce Comité dont il assure l'organisation, le secrétariat et la présidence. Il est tenu de communiquer aux Participants sur l'extranet dédié l'ordre du jour, les documents préparatoires et les avis, et les décisions prises par l'Administrateur dans des délais permettant leur examen et leur mise en œuvre.

Les Participants doivent utiliser exclusivement l'extranet dédié dans le cadre strict de leur activité professionnelle et ne doivent pas communiquer son URL à des tiers non-autorisés.

Ce Comité de Pilotage abordera les sujets suivants (liste non exhaustive) :

- Suivi de production et de l'exploitation de la Plateforme du FNC-RF ;

- Suivi des indicateurs agrégés de performance et de bonne utilisation de la Plateforme du FNC-RF ;
- Proposition d'évolution fonctionnelle ;
- Proposition de modification des présentes CGU ;
- Planification des évolutions fonctionnelles/techniques de la Plateforme ;
- Examen des Incidents majeurs et des mesures correctives mises en œuvre ;
- Suivi de la conformité aux obligations légales et réglementaires applicables ;
- Mise en place et évolution d'un corpus de règles et autres bonnes pratiques d'utilisation du FNC-RF.

8.2. Modalités de vote au sein du Comité de Pilotage en cas d'absence de consensus

Les délibérations sont prises à la majorité simple des voix exprimées par les Participants actifs présents ou représentés. En cas de partage égal des voix, la voix du Président (Administrateur) est prépondérante.

Les Participants en consultation disposent d'une voix consultative mais ne participent pas au vote.

Les délibérations relatives aux modifications des CGU ou aux évolutions majeures de la Plateforme requièrent une majorité qualifiée des deux tiers des Participants actifs présents ou représentés.

Article 9. Support, évolutions et exploitation

9.1. Assistance aux Participants

L'Administrateur met à disposition des Participants une assistance qui comprend plusieurs niveaux selon le type de demande ou la gravité de l'Incident rencontré. Le contenu de cette assistance ainsi que ses modalités d'accès sont précisés en Annexe 1.

Avant de solliciter ce service d'assistance, le Participant consulte la documentation mise à sa disposition par l'Administrateur. La mise à jour de cette documentation est en outre assurée par l'Administrateur, qui s'engage à en informer les Participants dès sa publication.

9.2. Gestion des évolutions de la solution

Ce processus est décrit à l'Annexe 1. Toute évolution majeure est soumise à la validation préalable du Comité de Pilotage.

9.3. Gestion des Incidents ou Anomalies

Ce processus est décrit à l'Annexe 1.

9.4. Maintenance corrective et adaptative

Les obligations de l'Administrateur en matière de maintenance corrective et adaptative de la Plateforme centrale sont décrites à l'Annexe 1.

Il est rappelé que les montées de versions MISP, gérées par le projet MISP en charge du maintien du code open source, peuvent induire des effets de bord sur le déroulement des processus (mode MISP et API). La stratégie de maintenance, devant être respectée par l'ensemble des Participants, sera soumise à la validation du Comité de Pilotage.

L'Administrateur s'engage à informer les Participants en amont de toute montée de version susceptible d'impacter leurs systèmes locaux. Les Participants s'engagent à garantir la cohérence entre leur SI et le SI de l'Administrateur, notamment pour les montées de version de MISP.

9.5. Recette d'homologation

Les recettes communautaires permettent à l'ensemble des Participants de valider en commun le bon fonctionnement des nouvelles versions de FNC-RF ainsi que la bonne interopérabilité des applications propres aux Participants s'interfaçant avec FNC-RF.

Des périodes de recette communautaire sont organisées par l'Administrateur en concertation avec les membres du Comité de Pilotage. En fonction des dispositions prévues dans la stratégie de maintenance validée par le Comité de Pilotage, la fin de recette peut donner lieu à établissement par l'Administrateur d'un procès-verbal, à valider par les membres du Comité de Pilotage, préalablement à la mise en production.

Les créneaux retenus pour effectuer les mises en production, ainsi que les recettes communautaires, sont fixés par l'Administrateur après avis du Comité de Pilotage sur la base des calendriers de production, de façon à limiter au maximum l'impact sur l'activité du FNC-RF.

L''environnement d'homologation reste disponible pour la réalisation des campagnes de test, notamment en cas de montée d'une version majeure MISP.

Pour des raisons d'organisation, et dans le cas d'accompagnement par l'Administrateur, le Participant souhaitant réaliser les tests doit s'annoncer auprès de l'Administrateur en respectant un délai de préavis fixé par le Comité de pilotage.

9.6. Plan de continuité de l'activité

Le plan de continuité de l'activité (PCA), ainsi que les procédures afférentes, sont élaborés par l'Administrateur qui les soumet pour validation au Comité de Pilotage. L'Administrateur s'engage à communiquer aux Participants les modalités de déclenchement du PCA et les délais de reprise d'activité prévus.

9.7. Demande d'action sensible par le Participant

Un Participant peut demander à l'Administrateur les demandes sensibles suivantes :

- suppression ou modification - à titre exceptionnel - de données enregistrées dans la Plateforme, en situation de contingence reconnue par l'Administrateur ;
- création, modification ou suppression de comptes utilisateurs ;
- modification des droits d'accès attribués aux comptes utilisateurs ;
- transmission ou validation de données complémentaires ou justificatives ;
- demande de suspension ou de réactivation d'un raccordement technique ;
- validation d'évolutions techniques ou fonctionnelles impactant la sécurité ou la disponibilité du dispositif ;
- modification du formulaire de mise à jour du référentiel de BIC
- modification de ou des adresses IP du Participant dans les référentiels de l'Administrateur, à l'aide du formulaire de raccordement en mode modification.
- toute autre action identifiée comme sensible par le Comité de Pilotage et communiquée aux Participants.

Le Participant renseigne dans le formulaire de Raccordement les noms et coordonnées des personnes habilitées à adresser ces demandes (les « Responsables métier fraude »). Le Participant s'engage par ailleurs à communiquer à l'Administrateur, dans les plus brefs délais, toute modification de cette liste des contacts autorisés.

L'Administrateur se réserve le droit de refuser une demande en provenance d'une personne non présente dans cette liste des contacts autorisés communiquée par le Participant. En cas de refus, l'Administrateur en informe immédiatement le Participant concerné.

Article 10. Tarification - Facturation

10.1. Tarification

Chaque année, l'Administrateur adresse à chaque Participant une lettre d'information notifiant les éléments relatifs à la tarification de la Plateforme du FNC-RF. Ces éléments se fondent sur les termes décrits dans l'arrêté mentionné au VII du L.521-6-1 du code monétaire et financier.

10.2. Modalités de facturation

Les factures sont établies en euros et adressées au correspondant du payeur désigné, par le Participant, dans le bulletin de facturation.

La facture est payable, dans un délai de trente (30) jours à compter de sa date de réception, nette et sans escompte, en totalité et selon les modalités indiquées dans le bulletin de facturation.

En application des dispositions légales, le Participant est automatiquement redevable, en cas de retard de paiement, d'une pénalité exigible le jour suivant la date de règlement prévue. Le taux de cette pénalité est égal au taux d'intérêt appliqué par la Banque centrale européenne à son opération de refinancement la plus récente majoré de dix (10) points de pourcentage. Le taux applicable pendant le premier semestre de l'année concernée est le taux en vigueur au 1er janvier de l'année en question. Pour le second semestre de l'année concernée, il est le taux en vigueur au 1er juillet de l'année en question. Le Participant est également redevable d'une indemnité forfaitaire pour frais de recouvrement, d'un montant de quarante (40) euros.

Lorsque le Participant relève du secteur public, en application des dispositions légales, il est automatiquement redevable, en cas de retard de paiement, d'intérêts moratoires exigibles le jour suivant la date de règlement prévue. Ces intérêts moratoires, dont le taux est égal au taux d'intérêt appliqué par la Banque centrale européenne à ses opérations principales de refinancement les plus récentes, en vigueur au premier jour du semestre de l'année civile au cours duquel les intérêts moratoires ont commencé à courir, majoré de huit (8) points de pourcentage. L'Adhérent est également redevable d'une indemnité forfaitaire pour frais de recouvrement, d'un montant de quarante (40) euros. Les intérêts moratoires et l'indemnité forfaitaire pour frais de recouvrement sont payés dans un délai de quarante-cinq (45) jours suivant la mise en paiement du principal.

Le payeur de la prestation n'est pas nécessairement le Participant. Le payeur doit cependant être obligatoirement une personne morale.

Le Participant doit communiquer à l'Administrateur dans le bulletin de facturation l'ensemble des informations permettant de procéder au paiement. En cas de changement affectant ces informations, le participant notifie ces éléments sans délai à l'Administrateur en lui soumettant un nouveau bulletin de facturation intégrant la mise à jour des données nécessaires à l'exécution de ces paiements.

À compter du 1er septembre 2026, les factures sont transmises sous forme dématérialisée par la Plateforme de Dématérialisation Partenaire (PDP), accessible à l'adresse suivante :

https://app.cecurity.com/platform/login

Pour les Adhérents relevant du secteur public, les factures sont transmises sous forme dématérialisée, par le Portail Public de Facturation (PPF), accessible à l'adresse suivante :

https://chorus-pro.gouv.fr

Article 11. Responsabilités des parties

11.1. Responsabilités de l'Administrateur

L'Administrateur est responsable du code informatique dont il est l'auteur dans le cadre de la mise en production du FNC-RF. À ce titre, il s'engage à maintenir les composants logiciels conformes à l'état de l'art et à assurer leur mise à jour régulière.

L'Administrateur s'engage à mettre en œuvre les contrôles relatifs à l'utilisation du FNC-RF qui auront fait l'objet d'une approbation en Comité de Pilotage. Ces contrôles peuvent porter sur le respect de conformités réglementaires ou bien de bonnes pratiques émanant du Comité de Pilotage.

L'Administrateur est responsable du calcul et de la diffusion des résultats relatifs aux indicateurs de performance définis au sein du Comité de Pilotage.

L'Administrateur ne pourra pas être tenu responsable de la mise à disposition d'informations erronées, alimentées par un Participant, sous réserve que ces erreurs soient en dehors du champ des contrôles que l'Administrateur est lui-même chargé d'effectuer, ces derniers étant déterminés par l'Administrateur après avis du Comité de Pilotage.

Les informations communiquées sont celles qui figurent dans le fichier à la date et à l'heure de l'interrogation. Elles peuvent être modifiées à tout instant à la suite de la prise en compte des déclarations et modifications transmises par les Participants.

L'Administrateur ne peut être tenu pour responsable des conséquences dommageables qui pourraient résulter d'omissions ou d'informations inexactes, incomplètes ou périmées transmises par les Participants.

La responsabilité de l'Administrateur pour interruption de fonctionnement de ses équipements informatiques ou des liaisons télématiques est engagée selon les règles de droit commun ; elle est dégagée en cas de force majeure mettant l'Administrateur dans l'impossibilité de fournir le service proposé. La responsabilité de l'Administrateur ne peut également être engagée en cas d'évènements ou Incidents indépendants de sa volonté tels que grève, troubles sociaux ou incendie.

L'Administrateur s'engage à informer les Participants de toute évolution des normes et standards utilisés et plus généralement de toute évolution fonctionnelle ou technique des services proposés sur le FNC-RF.

11.2. Responsabilités du Participant

Le Participant s'engage à renseigner l'ensemble des bulletins et formulaires mentionnés à l'article 3, ainsi qu'à notifier sans délai à l'Administrateur lorsque qu'ils ne sont plus à jour. Le cas échéant, le Participant est responsable de transmettre à l'Administrateur sous un délai d'une semaine les bulletins et les formulaires devant faire l'objet d'une mise à jour.

Le Participant s'engage à notifier par écrit à l'Administrateur tout changement d'adresse de facturation.

Le Participant actif réalisant des modifications sur son Système local sans s'être assuré de leur compatibilité avec le fonctionnement du FNC-RF, en assume seul les conséquences dommageables de celles-ci vis-à-vis des autres Participants et des tiers.

Le Participant est responsable :

- des données qu'il enregistre dans la Plateforme du FNC-RF ;
- de la mise en œuvre des infrastructures et traitements leur permettant d'interagir avec la Plateforme centrale

Toutefois, le Participant actif ne peut être tenu pour responsable des conséquences dommageables qui pourraient résulter d'omissions ou d'informations inexactes, incomplètes ou périmées qui ont été mises à disposition par un autre Participant sur la Plateforme du FNC-RF.

Le Participant exploite le contenu des données partagées sur la Plateforme du FNC-RF sous sa seule responsabilité et est seul responsable des modifications qu'il apporte aux données après les avoir récupérées dans son système d'information local.

Le Participant, dans le cadre de sa participation au FNC-RF, est responsable d'assurer sa conformité aux différentes règles et lois auxquelles il est assujetti. Il s'engage également à respecter les bonnes pratiques émanant du Comité de Pilotage, ainsi qu'à répondre de manière diligente aux requêtes en provenance de l'Administrateur qui visent à assurer le respect de ces bonnes pratiques par l'ensemble des Participants.

Le Participant s'engage en particulier à respecter les obligations suivantes :

- l'usage des données du FNC-RF est réservé à ses seuls besoins internes tels que définis par article L521-6-1 du code monétaire et financier (ou ceux de son groupe tel que défini à l'article 4.2) ;
- la diffusion des données par le Participant actif à des tiers est interdite, à l'exception des prestataires techniques pour lesquels le Participant actif a défini contractuellement les limites d'usage et les exigences de sécurité nécessaires à l'application de l'article L 521-6-1 du code monétaire et financier et des présentes CGU ;
- le Participant s'abstient de tout usage des données contenues dans le FNC-RF contraire aux lois et règlements en vigueur en France. Il lui est notamment rappelé que les informations contenues dans le FNC-RF sont couvertes par le secret professionnel.

Lorsque le Participant intervient en qualité de Chef de file, chacun des établissements qu'il représente est tenu aux mêmes obligations que le groupe dans le cadre de l'exécution des présentes CGU. Le chef de file doit s'assurer du respect de la présente convention par les établissements représentés et reste responsable devant la Banque de France de l'exécution de ces obligations.

Le Participant intervient en qualité de Chef de file s'engage à informer les établissements qu'il représente des obligations qui pèsent sur eux en application de la présente convention.

Lorsque le Participant confie l'exploitation informatique à un prestataire de service informatique, ce dernier en qualité de sous-traitant, n'est exonéré d'aucune des responsabilités susvisées.

Article 12. Force majeure

Chacune des Parties est dégagée de toute responsabilité si l'inexécution de ses obligations résulte d'un cas de force majeure tel que défini par la loi et les tribunaux.

Sont expressément considérés comme des cas de force majeure le conflit social interne ou externe ainsi que le dysfonctionnement ou l'interruption totale ou partielle des réseaux de communications électroniques dont les parties n'ont pas la maîtrise.

En présence d'un cas de force majeure, si l'empêchement est temporaire, les parties fournissent leurs meilleurs efforts pour poursuivre l'exécution des présentes.

La partie qui invoque le cas de force majeure doit, sans délai et par tout moyen, informer l'autre ou les autres partie(s) de son impossibilité à exécuter ses obligations et s'en justifier auprès de celle(s)-ci.

Article 13. Secret professionnel

L'Administrateur est délié du secret professionnel pour la communication des informations nominatives contenues dans le FNC-RF, aux Participants.

Les informations communiquées par l'Administrateur ainsi que les états et documents provenant de leur traitement sont couverts par le secret professionnel auquel sont soumis les Participants ainsi qu'à leur personnel.

Les Participants ne doivent pas faire état auprès de tiers non autorisés des renseignements obtenus auprès de l'Administrateur. Ils s'engagent à respecter et à faire respecter, de façon absolue, cette obligation au secret et à prendre toutes mesures nécessaires à cet effet. Ils doivent interdire tout accès au FNC-RF à des tiers non autorisés à partir des différents modes de raccordement.

Les Participants doivent utiliser exclusivement l'extranet dédié (cf. Article 8) dans le cadre strict de leur activité professionnelle et ne doivent pas communiquer son URL à des tiers non autorisés.

Article 14. Protection des données à caractère personnel

Les termes ci-après relatifs au traitement des données à caractère personnel qui ne sont pas expressément définis aux présentes CGU ont le sens qui leur est donné par le Règlement (UE) 2016/679 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 ("RGPD").

14.1. L'Administrateur et les Participants sont responsables de traitement, chacun en ce qui les concerne, à l'égard de leurs propres salariés, collaborateurs, agents ou tous autres préposés ou personnels intervenant dans l'exécution des présentes du respect de ces dispositions et s'engagent à les informer de la teneur de leurs droits en la matière ainsi que des modalités d'exercice de ceux-ci. Les données à caractère personnel recueillies sur les contacts métier et technique au sein du bulletin d'adhésion et de renseignement sont collectées dans le cadre de l'exécution des présentes CGU. Elles sont nécessaires pour la gestion de l'adhésion et de la participation au FNC-RF, notamment pour la tenue d'un annuaire des correspondants des Participants, et font l'objet d'un enregistrement dans un fichier informatisé par l'Administrateur. Elles sont conservées par l'Administrateur jusqu'à l'envoi, par le Participant, d'un nouveau bulletin d'adhésion et de renseignement, d'une liste des Correspondants ou encore d'un mandat de prélèvement mis à jour, puis, à compter de la réception de cet envoi, pendant un délai maximal de trois (3) mois. Les données relatives au(x) contact(s) métier ainsi qu'au(x) contact(s) technique sont destinées à être partagées avec les autres Participants dans le cadre d'un annuaire des correspondants. Ces données ne sont pas traitées à des fins de prospection commerciale.

Conformément aux dispositions en vigueur, les personnes désignées au sein des différents bulletins et formulaires mentionnés à l'article 3 et inscrites dans l'annuaire des correspondants des participants disposent d'un droit d'accès, de rectification et de portabilité des données les concernant qui peut être exercé en contactant : Banque de France - S1D 1946 DESP COP, 1 Rue la Vrillière -75049 PARIS CEDEX 01. L'exercice des droits d'opposition, de limitation du traitement ainsi que l'exercice du droit de définir des directives relatives au sort de ses données à caractère personnel après son décès sont effectués auprès du Participant concerné. Les personnes désignées sur ces formulaires peuvent également effectuer une réclamation auprès de la Commission Nationale de l'Informatique et des Libertés.

L'Administrateur et chaque Participant assument toutes les conséquences pouvant résulter du non-respect de ces dispositions entre eux et à l'égard de la CNIL et de tout tiers.

14.2 Conformément à la réglementation en vigueur, les Participants ont l'obligation de transmettre à l'Administrateur les données à caractère personnel telles que définies à l'article L521-6-1 du code monétaire et financier et par l'arrêté mentionné au VI du L.521-6-1 du code monétaire et financier, portant sur les personnes qui ont commis ou qui sont suspectées d'avoir commis une fraude détectée par le Participant dans le cadre de son activité. Les données issues du fichier ne peuvent être utilisées par les Participants que pour les finalités prévues par la réglementation et rappelées en préambule du présent document.

L'Administrateur et chaque Participant s'engagent à respecter les dispositions du Règlement (UE) 2016/679 et de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, notamment celles qui sont relatives à la sécurité des données à caractère personnel et à l'information des personnes physiques concernées.

L'Administrateur est responsable de traitement en ce qui concerne la gestion du fichier.

Le Participant est responsable de traitement pour les données personnelles qu'il détient dans le cadre de ses activités. Il est responsable de traitement en ce qui concerne les actions qu'il effectue sur les données personnelles provenant du fichier et il est responsable des instances locales du fichier.

Chaque Participant reste responsable de traitement à l'égard de ses clients, et s'engage à les informer de la teneur de leurs droits en la matière ainsi que des modalités d'exercice de ceux-ci.

L'information des personnes sur l'existence de ce fichier est de la responsabilité des Participants à l'égard de leurs clients.

La personne physique concernée dispose d'un droit d'accès aux données enregistrées dans le fichier auprès de son PSP teneur de compte qui peut s'exercer selon des modalités à définir par chaque Participant.

Le droit de rectification portant sur les données contenues dans le fichier s'effectue auprès du Participant teneur de compte, y compris lorsqu'il est exercé sur le fondement d'une décision de justice ordonnant la rectification des informations relatives à la personne concernée.

En présence d'un groupe, chacun des établissements représentés est tenu aux mêmes obligations que le chef de file dans le cadre de l'exécution des présentes CGU. Le chef de file s'assure que ces établissements respectent les obligations des présentes CGU et présentent les mêmes garanties quant à la mise en œuvre des mesures techniques et organisationnelles prévues afin que le traitement réponde aux exigences du Règlement (UE) 2016/679 susvisé.

Pour s'assurer et être en mesure de démontrer que les traitements sont effectués en conformité avec les dispositions légales et réglementaires applicables, l'Administrateur et les Participants mettent en œuvre les mesures techniques et organisationnelles appropriées pour protéger les données contre une destruction fortuite ou illicite, une perte accidentelle, une altération, une divulgation ou un accès non autorisé. Ces mesures assurent un niveau de sécurité adapté aux risques liés aux traitements et à la nature des données protégées.

En cas de violation de données à caractère personnel, au sens de l'article 33 du Règlement (UE) 2016/679 du 27 avril 2016 susvisé, l'Administrateur et les Participants mettent en œuvre la procédure prévue à l'Annexe 6. Les parties notifient en même temps que l'autorité de contrôle les autres parties de toute violation de données à caractère personnel. Cette notification est accompagnée de toute documentation utile afin, le cas échéant, de permettre aux parties de notifier cette violation à l'autorité de contrôle.

Dans ces conditions, la notification de la violation à l'autorité de contrôle est effectuée par l'Administrateur pour les violations relatives à la gestion de la Plateforme centralisée et par chaque participant pour les violations relatives aux instances locales de la Plateforme et aux violations intervenant dans leur processus internes d'identification des données personnelles inscrites dans le fichier

L'Administrateur et chaque Participant assument toutes les conséquences pouvant résulter du non-respect de ces dispositions entre eux et à l'égard de la CNIL et de tout tiers.

Les Participants s'engagent, pour eux-mêmes ainsi que, le cas échéant, pour les entités appartenant à leur groupe tel que défini à l'Article 6, à ne pas utiliser les données contenues dans le FNC-RF à d'autres fins que celles prévues par les textes et notamment à des fins de prospection commerciale. Ils doivent respecter et faire respecter cette obligation, par leurs mandataires et préposés et, le cas échéant, par ceux des entités appartenant à leur groupe.

Les données à caractère personnel portant sur les personnes physiques sont conservées dans le FNC-RF jusqu'à l'expiration des délais de prescription et d'archivage définis dans l'arrêté mentionné à l'article L 521-6-1 du Code Monétaire et Financier.

Les coordonnées du délégué à la protection des données de la Banque de France, Administrateur, sont *1200-DPD-delegue-UT@banque-france.fr*. Le Participant s'engage à communiquer au délégué à la protection des données de l'Administrateur les coordonnées de son propre délégué à la protection des données dans les dix (10) jours calendaires suivant la date d'adhésion aux présentes CGU. Les coordonnées des délégués à la protection des données des Participants sont destinées à être partagées entre eux.

Article 15. Évolutions légales ou réglementaires

Le Participant reconnaît que les présentes CGU peuvent évoluer ou être ajustées compte tenu des évolutions des exigences légales ou réglementaires.

Le Participant ne peut en aucun cas prétendre au maintien des solutions techniques mises en place lors de son adhésion aux présentes CGU, dès lors que leur modification est rendue nécessaire par une évolution légale ou réglementaire. L'Administrateur s'engage toutefois à informer les Participants dans des délais raisonnables afin de leur permettre d'adapter leurs systèmes et procédures.

Article 16. Correspondants

L'Administrateur et le Participant désignent chacun au moins un correspondant qui est l'interlocuteur dédié de l'autre et qui coordonne les actions relatives à l'exécution des présentes.

Le correspondant (métier fraude) du Participant est notamment chargé d'adresser sans délai à la Banque de France les bulletins et formulaires modifiés lorsque ces derniers ne sont plus à jour, comme précisé à l'article 4.1.

Le nom et les coordonnées des correspondants désignés sont précisés dans le bulletin d'adhésion et de renseignement, ainsi que celui de raccordement.

L'Administrateur et le Participant s'engagent à s'informer sans délai et par écrit de la désignation d'un nouveau correspondant et de tout changement affectant celui-ci. Toute modification implique le renvoi du document prévu à cet effet mis à jour afin de permettre à l'Administrateur de tenir à jour l'annuaire de contacts des Participants qu'il partage entre eux.

Article 17. Durée, révision et résiliation des conditions générales

17.1. Durée

Les présentes CGU prennent effet à compter de la date effective de l'adhésion conformément à l'Article 4 des présentes. Elles sont conclues pour une durée indéterminée.

17.2. Révision

Nonobstant les dispositions prévues à l'Article 15, les présentes CGU peuvent être révisées, après avis du Comité de Pilotage, dans les conditions prévues à l'Article 8, par l'Administrateur notamment dans les cas suivants :

- pour se conformer à une évolution législative ou réglementaire applicable ;
- pour mettre en œuvre une décision ou une instruction d'une autorité de supervision ou de régulation compétente ;
- pour répondre à un impératif de sécurité ou de continuité de service du dispositif, dûment justifié et communiqué aux Participants.

Ces modifications sont applicables, par principe, trois (3) mois après leur notification aux Participants. Sur demande des Participants ou à l'initiative de l'Administrateur, ce délai peut être soumis à la délibération du Comité de Pilotage et modifié par l'Administrateur.

Les notifications sont systématiquement adressées au correspondant désigné par les parties conformément à l'article 16.

17.3. Résiliation de la convention

17.3.1 Résiliation de la convention en cas de sortie d'un groupe

Les Participants qui ont adhéré à la Plateforme par l'intermédiaire d'un groupe peuvent, à tout moment, résilier la convention afin d'adhérer au fichier de manière indépendante tel que cela est mentionné à l'article 4.1.

Sauf demande explicite de rallongement du délai, la résiliation prend effet à l'issue d'un délai de trois (3) mois.

Si le Participant souhaitant sortir du groupe à la qualité de chef de file ou s'il a signé le formulaire de raccordement pour le compte du groupe, chaque Participant représenté doit prendre ses dispositions pour s'associer à un autre Participant de son groupe afin de continuer à remplir ses obligations légales vis-à-vis du FNC-RF ou devenir lui-même Participant. Dans ce cadre, le chef de file informe la Banque de France des

nouvelles dispositions prises pour chaque établissement représenté, avant la date de résiliation effective de la convention. Le délai de résiliation peut être prolongé en cas de besoin afin d'assurer la continuité de l'accès à la Plateforme par les Participants concernés.

17.3.2 Résiliation de la convention liée à une perte d'agrément

Le Participant informe l'Administrateur, dès qu'il a connaissance, d'évènements pouvant être de nature à affecter son statut le rendant éligible à participer au FNC-RF, tel que précisé au L.521-6-1 du Code Monétaire et Financier.

17.3.2.1 Perte d'agrément du Participant

Lorsqu'un Participant ne remplit plus les conditions d'accès, il en informe immédiatement l'Administrateur. La présente convention prend automatiquement fin à l'égard de l'établissement rattaché concerné à la date de prise d'effet du retrait d'agrément.

L'Administrateur confirme par courrier au Groupe Participant ainsi qu'à l'établissement rattaché concerné que l'habilitation de celui-ci est supprimée.

Lorsqu'un Participant représente un ou plusieurs autres établissements, il les informe au plus tôt de la résiliation de sa convention avec l'Administrateur. Chaque établissement représenté doit prendre ses dispositions pour s'associer à un autre Participant de son Groupe Participant afin de continuer à remplir ses obligations légales vis-à-vis du FNC-RF ou devenir lui-même Participant. Dans ce cadre, le Groupe Participant informe l'Administrateur des nouvelles dispositions prises pour chaque établissement représenté concerné, avant la date d'effet de la perte d'agrément du Participant.

17.3.2.2 Perte d'agrément du chef de file

Lorsque le chef de file n'a plus la qualité de prestataire de service de paiement, les présentes CGU prennent fin automatiquement, à la date de prise d'effet du retrait d'agrément, tant à son égard qu'à l'égard des établissements représentés, et la Banque de France confirme au chef de file par courrier que leur habilitation au fichier est supprimée.

En outre, en cas de retrait d'agrément du chef de file, chaque établissement représenté doit prendre ses dispositions pour s'associer à un autre Participant de son groupe afin de continuer à remplir ses obligations légales vis-à-vis du FNC-RF ou devenir lui-même Participant. Dans ce cadre, le chef de file informe la Banque de France des nouvelles dispositions prises pour chaque établissement représenté, avant la date d'effet de la perte d'agrément.

17.3.2.3 Perte d'agrément de l'établissement représenté

Lorsqu'un établissement représenté ne remplit plus les conditions d'accès au FNC-RF, le chef de file en informe immédiatement la Banque de France. Les présentes CGU prennent automatiquement fin à l'égard de l'établissement représenté concerné à la date de prise d'effet du retrait d'agrément et la Banque de France confirme par courrier au chef de file que l'habilitation de cet établissement est radié de la liste des Participants. Le chef de file en informe l'établissement représenté concerné.

18 Droit applicable - Langue - Attribution de compétence

Les présentes CGU sont soumises au droit français.

En cas de litige qui viendrait à naître entre les Participants ou entre les Participants et l'Administrateur à propos de l'exécution ou de l'interprétation des présentes CGU, chacun s'engage à coopérer avec diligence et bonne foi en vue de trouver une solution amiable.

Si toutefois, il n'est pas parvenu pas à un accord pour tout litige qui pourrait s'élever dans l'interprétation ou l'exécution des CGU, compétence est attribuée aux tribunaux de Paris

19 Sanctions

En cas de manquement du Participant à l'une quelconque des obligations mises à sa charge dans le cadre des présentes CGU, il peut être mis en demeure par l'Administrateur, par lettre recommandée avec demande d'avis de réception, de réparer ce manquement dans un délai proportionné à la nature du manquement lequel ne peut excéder 45 jours ouvrés à compter de la découverte du manquement.

Si, à l'issue de ce délai, le manquement n'est pas réparé, l'Administrateur peut par lettre recommandée avec avis de réception, notifier au Participant que ses accès au FNC-RF sont susceptibles d'être suspendus dans un délai d'une semaine à compter de la date d'envoi de la lettre recommandée susmentionnée, et ce pour une durée indéterminée.

L'Administrateur s'engage toutefois à rétablir l'ensemble des accès au Participant sous un délai d'une semaine lorsqu'il estime que le manquement est réparé.

Le Participant demeure tenu de régler toutes les sommes dues au titre des présentes dispositions jusqu'à la date effective de la résiliation.

En cas de résiliation imputable au Participant, celui-ci est également redevable, le cas échéant, de toutes sommes dues au titre de la facture de régularisation liée à la couverture des coûts du fichier adressée l'année suivant celle de la prise d'effet de la résiliation, quelle que soit la cause de celle-ci.

Dans l'hypothèse où le calcul destiné à vérifier la couverture des coûts complets du fichier engendrerait un avoir au bénéfice du groupe, la Banque de France lui adresserait le règlement correspondant par tout moyen approprié.

Par ailleurs, l'inobservation de dispositions légales et règlementaires ainsi que tout retard dans les déclarations sont passibles des sanctions prévues à l'article L. 612-39 du code monétaire et financier.

20 Signature électronique

Les Participants et l'Administrateur conviennent que les présentes CGU, y compris les différents bulletins et formulaires listés à l'article 3, l'ensemble étant considéré comme formant un tout indivisible, peut être conclu par voie électronique, dans les conditions suivantes :

- le signataire, personne physique, des présentes CGU est réputé être dûment habilité à représenter le Participant et à l'engager juridiquement. Le Participant veille à ce que la personne qui le représente, dans le cadre des présentes CGU, dispose des pouvoirs ou des délégations de pouvoirs et/ou de signature nécessaires. Le défaut du Participant dans la gestion de ces pouvoirs ou délégations de pouvoirs et/ou de signature ne pourra pas être opposé à l'Administrateur pour faire échec à la valeur juridique des présentes CGU ;
- la signature électronique utilisée résulte de l'usage d'un procédé fiable d'identification garantissant son lien avec les présentes CGU auxquelles elle s'attache ;
- la signature doit être une signature « avancée » reposant sur un certificat qualifié, conforme au règlement européen n° 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques (eIDAS) ;
- la signature électronique avancée satisfait aux exigences de l'article 26 du règlement précité, à savoir ;
  - être liée au signataire de manière univoque ;
  - permettre d'identifier le signataire ;
  - avoir été créée à l'aide de données de création de signature électronique que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif ; et
  - être liée aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable.

- un certificat de signature électronique de niveau qualifié est requis au minimum. Il appartient à l'une des catégories suivantes :
  - un certificat qualifié délivré par un prestataire de service de confiance qualifié répondant aux exigences du règlement susvisé ;
  - un certificat délivré par une autorité de certification, française ou étrangère, qui répond aux exigences équivalentes à l'annexe I du règlement susvisé.

- le certificat de signature utilisé doit respecter les exigences prévues par l'annexe I du règlement précité et permettre notamment de vérifier :
  - l'identité du signataire ;
  - l'appartenance du certificat du signataire à l'une des catégories de certificats précisées ci-avant ;
  - le respect du format de signature mentionné ci-après ;
  - le caractère non échu et non révoqué du certificat à la date de la signature ;
  - l'intégrité du document signé (non altéré ou modifié au cours du processus de signature).
- le format de signature utilisable est « PAdES ».

Pour apposer sa signature, le signataire utilise l'outil de signature de son choix.

Les présentes CGU ainsi signées électroniquement, que ce soit au moment de l'adhésion ou des éventuelles modifications ultérieures apportées à celle-ci, constitue l'original du document. Les Participants et l'Administrateur admettent la force probante du document signé électroniquement au même titre qu'un écrit signé sur support papier.

Les Participant et l'Administrateur font leur affaire personnelle de la conservation des présentes CGU dans des conditions de nature à garantir leur intégrité.

21 Dispositions finales

Le fait que l'une des parties n'ait pas exigé l'application d'une clause quelconque des CGU, que ce soit de façon permanente ou temporaire, ne peut en aucun cas être considéré comme une renonciation aux droits de cette partie découlant de ladite clause.

Si l'une quelconque des dispositions des présentes CGU est nulle au regard d'une règle de droit ou d'une loi en vigueur, elle est réputée non écrite mais n'entraîne pas la nullité des CGU.

Annexe 1 : Niveaux d'engagement de service (Service Level Agreement - SLA)

Introduction - Objectif

La présente annexe constitue l'engagement de service de l'Administrateur du FNC-RF.
Cet engagement de service a pour objectif d'exposer :

- les principes de fonctionnement des services entourant la Plateforme ;
- les modalités de gestion et d'exploitation de la Plateforme au sein de la communauté des Participants
- les niveaux de qualité et de disponibilité attendus dans la fourniture desdits services.

Le présent engagement de service peut faire l'objet de Demandes d'évolution à l'initiative de l'Administrateur ou des Participants. Les évolutions sont décidées par le Comité de Pilotage.

1. Parties impliquées dans l'engagement de service

Représentant de chaque partie

Acteur	Représentant
La Banque de France, Administrateur du FNC-RF	Cellule Opérationnelle des Paiements - DESP
Participant	Les contacts désignés dans le bulletin d'adhésion et de raccordement

2. Classes de services

Gestion de la disponibilité	22/24h et 7/7j 4 heures d'indisponibilité max par mois (hors vacation quotidienne de 00h à 2h
Surveillance	Monitoring test & Supervision des traitements batch Check quotidien au début d'activité et supervision par le Support
Gestion des Incidents	Prise en compte immédiat par le Support métier Délai de traitement selon la priorité de l'incident (Impact(x) Urgence) Communication en cas d'incidents majeurs
Gestion des changements	Montée des versions MISP et mise en place des évolutions demandées selon la stratégie de maintenance

3. Responsabilités de chaque partie

Chaque partie notifie sans délai les autres parties de tout changement impactant le cycle de vie de la Plateforme et/ou la qualité du service rendu.
Les participants sont tenus de respecter les spécifications de la Plateforme et la stratégie de maintenance.

4. Demandes d'assistance, traitement des Incidents et des Anomalies

L'Administrateur centralise et assure le suivi et le traitement des Demandes d'assistance, des Incidents et des Anomalies.

Une Demande d'assistance peut être faite auprès de l'Administrateur quel que soit le cas, ainsi que pour toute question concernant la gestion de la Plateforme.

5. Traitement des Demandes d'assistance

Dans le cadre d'une obligation de moyen, l'Administrateur intervient en support des équipes des Participants, soit pour un support ponctuel sur la mise en œuvre de FNC-RF, soit pour une assistance dans le cadre de la résolution d'un incident. Ces demandes prennent la forme de Demandes d'assistance.

- Demande par courriel à FNC-RF@banque-france.fr

Ces demandes d'assistance sont assorties d'un niveau d'importance :

- Faible : demande ayant des conséquences mineures sur l'activité des Participants ;
- Moyenne : demande portant sur un point gênant le travail des Participants, sans interrompre leur travail ;
- Haute : demande portant sur une interruption persistante des travaux des Participants ou un dysfonctionnement majeur de FNC-RF.

En fonction de leur importance, les demandes sont prises en compte dans le délai suivant, à compter de la réception, par l'Administrateur, du courriel de saisine (adressé directement par le Participant) :

	Délai de prise en compte
Niveau haut	< 2h
Niveau moyen	< 4h
Niveau faible	NA

Le calendrier des Jours Ouvrés est présenté au paragraphe 10 de la présente annexe. Les horaires au paragraphe 13.

Lors de l'entrée dans la communauté de FNC-RF d'un nouveau Participant, un plan de déploiement et de mise en œuvre de l'application est établi conjointement entre l'Administrateur et le nouveau Participant (selon le processus de raccordement en vigueur). Les modalités de mise en œuvre décidées dans ce plan se substituent au dispositif de traitement des demandes d'assistance décrites au présent paragraphe.

6. Traitement des Anomalies

Les signalements d'anomalie sont effectués par courriel à : fnc-rf@banque-france.fr, avec un niveau d'importance parmi :

- Faible : Anomalie ayant des conséquences mineures sur l'activité des Participants ;
- Moyenne : Anomalie gênant le travail des Participants, sans interrompre leur travail ;
- Haute : Anomalie interrompant de façon persistante les travaux des Participants ou provoquant un dysfonctionnement majeur de FNC-RF.

Le suivi des Anomalies et de leur correction sont instruits par L'Administrateur. Leur correction est validée par le Comité de Pilotage.

Dans le cadre d'une obligation de moyen, l'Administrateur corrige les anomalies déclarées par les Participants sur le code source du FNC-RF.

7. Traitement des Incidents et des alertes de sécurité

Les Participants signalent à l'Administrateur tout Incident susceptible d'impacter le fonctionnement d'ensemble du dispositif par :

- Demande par courriel à : fnc-rf@banque-france.fr

Les signalements d'Incidents sont assortis d'un niveau d'importance parmi :

- Faible : Incident ayant des conséquences mineures sur l'activité des Participants ;
- Moyenne : Incident gênant le travail des Participants, sans interrompre leur travail ;
- Haute : Incident interrompant de façon persistante les travaux des Participants ou provoquant un dysfonctionnement majeur de FNC-RF.

En fonction de leur importance, les Incidents sont pris en compte dans le délai suivant, à compter de la réception par l'Administrateur, de :

	Délai de prise en compte
Niveau Haut	< 2h
Niveau moyen	< 4 h
Niveau faible	NA

Le calendrier des jours ouvrés est présenté au paragraphe « 11. Calendrier ». Les horaires sont présentés au paragraphe « 13. Plages de support ».

L'Administrateur informe l'ensemble des Participants de l'Incident déclaré (Niveau Haut et Moyen).

Les Participants s'obligent à fournir à l'Administrateur tout élément technique permettant l'analyse de l'Incident. Les Participants coopèrent pleinement et sans réserve à la résolution de l'Incident.

Dans le cadre d'une obligation de moyen, l'Administrateur corrige les défauts du composant à l'origine de l'Incident.

Le Participant qui détecte une faille de sécurité pouvant entraîner une violation des données à caractère personnel en informe immédiatement l'Administrateur. Ce dernier alerte sans tarder les autres Participants et organise une réunion d'urgence du Comité de Pilotage.

8. Traitement des Demandes d'évolution

Les demandes d'évolution sont effectuées en Comité de Pilotage, et sont instruites par l'Administrateur.
Leur mise en œuvre est décidée par le Comité de Pilotage.

9. Prise en compte des modifications de FNC-RF par les Participants

Les modifications décidées par le Comité de Pilotage sont appliquées par l'Administrateur sur FNC-RF et par l'ensemble des Participants sur leurs systèmes locaux, lorsque nécessaire au fonctionnement général du dispositif, dans un délai décidé en Comité de Pilotage en fonction de l'ampleur des modifications nécessaires à leur mise en œuvre ou de difficultés signalées par un ou plusieurs Participants.
Les modifications susceptibles d'influer sur le fonctionnement d'ensemble de FNC-RF font l'objet d'une phase de recette communautaire dont l'organisation est soumise au Comité de Pilotage par l'Administrateur.

10. Calendrier

Les Jours ouvrés s'entendent hors samedis, dimanches et jours fériés. Les jours fériés sont définis à l'Article 2 des CGU de participation à FNC-RF.

11. Ouverture du service et disponibilité

Plages d'ouverture du service	22 h/24, 7 jours / 7 , 365 jours / 365 [coupure entre 0h00 et 2h00]
RTO - Durée maximale d'interruption	Lundi à Vendredi (hors jours fériés), entre 07h30 et 18h : 4 heures En dehors de ces plages : • Pas d'engagement de remise en condition opérationnelle • La remise en état se fait au plus tard 4h après retour dans la plage horaire
RPO - Durée maximale de perte de données	24

12. Supervision

Une surveillance de la Plateforme FNC-RF sera mise en place dès le premier jour d'exploitation en production

- Morning tests et surveillance des traitements batch par les services techniques
- Vérification du bon fonctionnement au démarrage de l'activité du Support et supervision en journée.

13. Plages de support

Rôle	Plage horaire
Support	9h00 – 18h00

14. Mode dégradé

En cas d'interruption de service, aucune action technique n'est envisagée en central par l'Administrateur. Celui-ci informe par courriel l'ensemble des Participants de la reprise du service:

- Participant en mode MISP : reprise de la synchronisation en mode nominal
- Participant en mode API : les appels effectués sur la plage d'indisponibilité sont à rejouer.

Annexe 2 : Surveillance de l'utilisation de la Plateforme FNC-RF

Des statistiques et indicateurs sont calculés par l'Administrateur, avec pour certains d'entre eux l'exploitation de données transmises par les Participants.

Ces statistiques et indicateurs permettent ;

1. De s'assurer que les Participants utilisent la Plateforme FNC-RF dans le respect des exigences règlementaires, des CGU et des règles d'usage convenues avec les Participants dans le cadre du Comité de Pilotage ;

2. D'évaluer l'efficacité du dispositif dans la lutte contre la fraude.

La liste et les modalités de calcul de ces statistiques et indicateurs est validée par le Comité de Pilotage.

Le cas échéant, le Participant s'engage à fournir les données complémentaires, non présentes dans la Plateforme FNC-RF, selon les modalités prévues et validées par le Comité de Pilotage.

L'Administrateur se réserve le droit de solliciter des éléments justificatifs de la part d'un Participant s'il estime que les statistiques et indicateurs concernant le Participant font apparaitre un usage anormal de la Plateforme FNC-RF.

Annexe 3 -4-5 : Les règles métier ainsi que les Spécifications Externes sont mises à disposition sur l'extranet confidentiel de la Banque de France.

Annexe 6 : Procédure en cas de violations de données à caractère personnel

1. Notification à l'autorité de contrôle

En sa qualité de responsable de traitement, l'Administrateur effectue la notification à l'autorité de contrôle conformément à l'article 33 du RGPD.

Le Participant notifie à l'Administrateur toute violation de données à caractère personnel par tout moyen (courriel à FNC-RF@banque-france.fr). Cette notification est accompagnée de toute documentation utile afin, le cas échéant, de permettre à l'Administrateur de notifier cette violation à la CNIL.

La notification du Participant à l'Administrateur contient au moins :

- la description de la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de dossiers concernés par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- le nom et les coordonnées du délégué à la protection des données ou du point de contact chez le Participant auprès duquel des informations supplémentaires peuvent être obtenues ;
- la description des conséquences probables de la violation de données à caractère personnel ;
- la description des mesures prises ou proposées pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Si, et dans la mesure où il n'est pas possible de fournir toutes ces informations en même temps, les informations peuvent être communiquées de manière échelonnée sans retard indu.

2. Communication aux personnes concernées

Le Participant détenteur de comptes communique la violation de données à caractère personnel aux personnes concernées dans les conditions de l'article 34 du RGPD. Les parties s'informent mutuellement des communications réalisées ou à réaliser.