

SOMMAIRE

CONDITIONS GÉNÉRALES COMMUNES AU CONTRAT.....	2
ARTICLE 1 : OBJET	2
ARTICLE 2 : CLIENTÈLE CONCERNÉE.....	2
ARTICLE 3 : MOYENS NÉCESSAIRES À L'UTILISATION DU SERVICE	2
ARTICLE 4 : ACCÈS AU SERVICE – SÉCURITÉ DU SYSTÈME	2
4.1 – Accès au Service	2
4.2 – Sécur'Pass.....	3
4.3 – Principes de sécurité	3
4.4 – Accès au compte de paiement et initiation de paiement.....	3
ARTICLE 5 : SPÉCIFICITÉS DE CERTAINES FONCTIONNALITÉS	3
5.1 – Souscription aux services.....	3
5.2 – Virements.....	3
5.3 – Service d'agrégation de comptes (sous réserve de disponibilité)	4
5.4 – Catégorisation de dépenses et de revenus.....	4
5.5 – Localisation des commerçants auprès desquels le Client a effectué une opération de paiement :.....	4
5.6 – Fonctionnalités de pilotage de la carte.....	4
5.7 – Abonnement à des produits offrant des alertes sur la situation du compte par SMS	4
5.8 – Opérations sur instruments financiers et autres titres	4
ARTICLE 6 : RESPONSABILITÉS.....	4
6.1 – Responsabilité de la Banque.....	4
6.2 – Responsabilité de l'Abonné	5
ARTICLE 7 : INFORMATIONS DIVERSES.....	5
ARTICLE 8 : RÈGLES DE PREUVE.....	5
ARTICLE 9 : TARIFICATION DU SERVICE	5
ARTICLE 10 : MODIFICATION DES CONDITIONS GÉNÉRALES ET LES CONDITIONS TARIFAIRES.....	5
10.1 – Modifications à l'initiative de la Banque	5
10.2 – Modifications imposées par des textes législatifs ou réglementaires.	5
ARTICLE 11 : DURÉE DE L'ABONNEMENT – RÉSILISATION OU SUSPENSION	6
ARTICLE 12 : PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL	6
ARTICLE 13 : RÉCLAMATIONS - MÉDIATION	6
ARTICLE 14 : LOI APPLICABLE – COMPÉTENCE - LITIGES	6

CONTRAT D'ABONNEMENT AU SERVICE INTERNET CYBERPLUS (conditions générales)

CONDITIONS GÉNÉRALES COMMUNES AU CONTRAT

a) BANQUE POPULAIRE OCCITANE

Société anonyme coopérative de Banque Populaire à capital variable, régie par les articles L.512-2 et suivants du Code Monétaire et Financier et l'ensemble des textes relatifs aux Banques Populaires et aux établissements de crédit - Intermédiaire en assurance inscrit à l'ORIAS sous le N° 07 022 714 - Immatriculée au Registre du commerce et des sociétés sous le numéro SIREN RCS TOULOUSE 560 801 300, ayant son siège social 33-43 avenue Georges Pompidou à Balma (31130).

Adresse mail : contact@occitane.banquepopulaire.fr.

Tout renseignement relatif à l'exécution de la présente convention ou à une contestation peut être obtenu en téléphonant au numéro suivant : 05 81 22 00 00 (Numéro non surtaxé)

b) Les coordonnées de l'autorité de contrôle compétente sont les suivantes : Autorité de Contrôle Prudentiel et de Résolution, 4 place de Budapest CS92459 75436 PARIS CEDEX 9

c) La liste des établissements de crédit et plus généralement celle des prestataires de services de paiement habilités peut être consultée sur le site de la Banque de France (<http://www.banque-france.fr>).

ARTICLE 1 : OBJET

L'abonnement au service de banque à distance CyberPlus de la Banque (ci-après dénommé le « Service ») permet au client abonné (ci-après « l'Abonné ») d'accéder à un ensemble de services rendus par la Banque, utilisant les nouvelles technologies (internet, téléphone...), pour consulter et/ou réaliser à distance, tout ou partie, des opérations sur le ou les compte(s) bancaire(s) ouvert(s) dans les livres de la Banque. L'Abonné peut ainsi obtenir des informations relatives au fonctionnement de son ou ses comptes, ainsi que diverses informations liées directement ou indirectement à l'activité bancaire. Selon la formule d'abonnement, il permet également à l'Abonné d'effectuer diverses opérations (notamment virements...) selon les conditions contractuelles.

Sont concernés par le Service, les comptes ouverts à la date d'adhésion audit Service et ceux ouverts ultérieurement.

Certaines opérations ou fonctionnalités peuvent, en fonction du canal ou du type de terminal utilisé ne pas être accessibles au moment de l'adhésion à CyberPlus. Les nouvelles fonctionnalités seront progressivement mises à disposition.

La Banque se réserve le droit de modifier le contenu de CyberPlus, en vue d'en améliorer la qualité, notamment par l'adjonction de nouvelles fonctionnalités. Dans une telle hypothèse, l'Abonné sera informé des éventuelles modifications du coût de fonctionnement.

ARTICLE 2 : CLIENTÈLE CONCERNÉE

Le Service est ouvert aux personnes physiques majeures capables, aux personnes physiques en sauvegarde de justice sans mandataire spécial, en curatelle simple avec l'accord de leur curateur, aux mineurs autorisés par leur représentant légal. En cas de compte joint, l'un et/ou l'autre titulaire peuvent être abonnés au Service. Chaque co-titulaire disposera de ses propres identifiant et mot de passe.

Les représentants légaux sont admis à effectuer des opérations sur les comptes de leurs enfants mineurs. Chaque représentant légal reconnaît que l'utilisation des identifiant et mot de passe, faite par un des représentants légaux du mineur, est réputée avoir reçu l'accord de l'autre. Dans l'hypothèse où un représentant légal s'oppose à ce mode de fonctionnement, il devra adresser un courrier recommandé avec avis de réception ou remis en main propre contre décharge à son agence gestionnaire du compte. Le Service sera alors résilié par la Banque pour le ou les comptes du ou des mineur(s) concerné(s).

Le cas échéant, l'Abonné peut conférer à un tiers une procuration spécifique sur un ou plusieurs de ses comptes et/ou contrats, ce

tiers devant lui-même adhérer au Service CyberPlus afin de disposer de ses propres identifiant et mot de passe.

ARTICLE 3 : MOYENS NÉCESSAIRES À L'UTILISATION DU SERVICE

L'abonnement au service CyberPlus de la Banque repose sur l'utilisation du réseau Internet et d'un terminal permettant cet accès : ordinateur, smartphone ou tablette et objets connectés à ces derniers. L'Abonné devra s'être procuré un accès au réseau Internet avant la mise en place du Service. Il devra également disposer d'un logiciel de navigation compatible dont les fonctions JavaScript et Cookies sont activées. La liste de ces navigateurs est accessible en ligne sur le site Internet de la Banque.

L'Abonné fait son affaire personnelle de l'acquisition ou de la location, de l'installation et de la connexion, de l'entretien et de la garde du matériel et de tous moyens techniques, accès aux réseaux ou logiciels tels que ceux placés sous contrôle exclusif de la Banque Populaire. La Banque Populaire n'est pas responsable de l'évolution des logiciels, de leur mise à jour et du maintien des référencements.

ARTICLE 4 : ACCÈS AU SERVICE – SÉCURITÉ DU SYSTÈME

4.1 – Accès au Service

Le service CyberPlus est exclusivement réservé à l'Abonné utilisateur, signataire de la Convention.

L'Abonné dispose d'un identifiant qui lui est propre. L'accès au Service requiert l'utilisation de dispositifs d'authentification :

- Mot de passe,
- Code de sécurité mis à disposition par SMS,
- Lecteur d'authentification par carte à puce (Pass Cyberplus) associé à une carte bancaire et son code confidentiel,
- Certificat numérique matériel associé à son code confidentiel,
- Fonction d'authentification intégrée à l'application mobile et couplée à un code confidentiel (Sécur'Pass),
- Reconnaissance biométrique intégrée aux terminaux compatibles sur les plateformes Android & iOS (Apple),
- Tout autre dispositif que la Banque jugera adéquat.

L'Abonné a l'obligation de modifier son mot de passe à sa première connexion. Il peut ensuite le modifier à tout moment.

La Banque met en place un dispositif d'authentification de l'Abonné pour l'accès à son compte en ligne et la réalisation des opérations de paiement (virements), des opérations sensibles (ajout d'un compte de bénéficiaire, enregistrement ou modification d'un ordre de virement permanent...) par l'intermédiaire des services de Cyberplus.

Ce dispositif d'authentification mis en place par la Banque repose sur l'utilisation de la solution Sécur'Pass ou d'un autre dispositif, le cas échéant.

L'utilisation de ce dispositif d'authentification, nécessitant également la saisie d'un code spécifique d'authentification (ci-après « Code »), pourra être exigée par la Banque lors du premier accès aux services de Cyberplus et au moins tous les 90 jours. La saisie du Code pourra éventuellement être effectuée par l'Abonné en utilisant la fonction biométrique de son smartphone.

La Banque pourra appliquer des exceptions à la mise en place de ce dispositif d'authentification de l'Abonné dans les conditions et selon les limitations prévues par le Règlement délégué UE 2018/389 du 27 novembre 2017.

Ce dispositif d'authentification repose sur l'utilisation d'au moins deux éléments parmi les trois catégories suivantes : 1) une information que l'Abonné est seul à connaître (mot de passe, code secret, code PIN), 2) l'utilisation d'un appareil qui appartient à l'Abonné (téléphone portable, montre connectée, appareil dédié fourni par la Banque...), 3) une caractéristique personnelle qui est intimement liée à l'Abonné (empreinte digitale, reconnaissance faciale, vocale...).

L'Abonné doit utiliser les données de sécurité personnalisées et les dispositifs d'authentification mis en place par la Banque chaque fois qu'il en reçoit l'instruction, sous peine d'engager sa responsabilité.

Dans le cas où le dispositif d'authentification ferait l'objet d'une facturation par la Banque, le montant de cette tarification sera porté à la connaissance de l'Abonné conformément aux dispositions de l'Article 10 des présentes conditions générales.

En cas d'utilisation d'un dispositif d'authentification mis en place par la Banque, l'Abonné doit prendre toutes les mesures nécessaires afin d'éviter (i) la divulgation à des tiers non autorisés, et/ou (ii) la copie, et/ou (iii) toute utilisation non autorisée des facteurs d'authentification. La Banque s'assure que les données de sécurité personnalisées (mot de passe, Code et tout élément d'authentification appartenant aux trois catégories précitées) ne sont pas accessibles à d'autres personnes que celles autorisées par l'Abonné, sauf si ce dernier ne respecte pas les préconisations mentionnées au présent article ou relatives au dispositif d'authentification mis à sa disposition par la Banque.

Compte tenu de l'évolution nécessaire et régulière des moyens de sécurité, la Banque se voit expressément reconnaître par l'Abonné, sans recours possible de ce dernier contre la Banque, la possibilité, à tout moment et à effet immédiat, de modifier de façon unilatérale les conditions d'authentification nécessaires à l'accès aux services, ou de supprimer certains dispositifs d'authentification moyennant une information de l'Abonné par tout moyen au choix de la Banque.

4.2 – Sécur'Pass

Dans le cadre de son abonnement à CyberPlus, l'Abonné a accès à Sécur'Pass, dispositif d'authentification forte permettant notamment à l'Abonné, depuis l'application mobile de la Banque :

- d'accéder aux services de Cyberplus et à son compte de dépôt en ligne ;
- de sécuriser l'accès et l'utilisation de certains services ;
- de valider certaines opérations sensibles initiées depuis son espace personnel de banque à distance (site internet CyberPlus ou application mobile CyberPlus) ;
- de valider des opérations de paiement réalisées en ligne (virements) et à distance par carte bancaire (e-commerce) ;
- de s'authentifier lors de la souscription de produits et services commercialisés par la Banque par voie dématérialisée en ayant recours à un dispositif de signature électronique.

La liste des fonctionnalités offertes par Sécur'Pass est susceptible d'évolution. L'Abonné en est informé via l'application mobile ou via la documentation s'y rapportant.

Sécur'Pass complète ou se substitue, le cas échéant, aux autres modes d'authentification, en permettant à l'Abonné de bénéficier de possibilités étendues.

L'enrôlement à Sécur'Pass est effectué par l'Abonné par la saisie de certains numéros aléatoires de sa carte bancaire en cours de validité et active, ou par une demande formulée auprès d'un conseiller en agence. L'Abonné doit posséder un smartphone compatible et préalablement enrôlé, dont le numéro a été préalablement déclaré à la Banque en tant que téléphone de préférence. Afin d'utiliser Sécur'Pass, l'Abonné doit également activer le service à partir de son espace personnel de banque à distance accessible depuis l'application mobile. L'activation de Sécur'Pass nécessite la saisie d'un code PIN choisi par l'Abonné.

Le changement de smartphone initialement enregistré nécessitera l'enrôlement du nouvel appareil.

Le choix, l'enregistrement, la modification, la réinitialisation et la conservation du code PIN associé à Sécur'Pass sont de la responsabilité de l'Abonné. Il lui appartient notamment de veiller à le conserver strictement secret, au même titre que l'ensemble des identifiants/mot de passe liés à son espace personnel de banque à distance ou à ses moyens de paiement. La Banque n'a aucun accès à ce code PIN.

Il est conseillé à l'Abonné de changer son code PIN fréquemment, de ne pas choisir un code PIN simple aisément décelable par un tiers, et de ne pas choisir un code PIN identique à celui qu'il utiliserait déjà par ailleurs, par exemple, le code PIN associé à son smartphone ou à sa carte SIM, ou le code confidentiel lié à son accès à la banque à distance, ou le code associé à sa carte bancaire.

Lors de l'utilisation de Sécur'Pass, la saisie du code PIN pourra éventuellement être effectuée par l'Abonné en utilisant la fonction biométrique de son smartphone.

L'Abonné a la possibilité de désactiver le dispositif Sécur'Pass à tout moment. En cas de cession de son smartphone, il lui appartient de veiller à la désactivation et à la désinstallation préalable de l'application.

La désactivation de Sécur'Pass est susceptible d'empêcher l'accès à certains services nécessitant le recours à une authentification forte, ou d'entraîner l'application d'exigences ou de délais complémentaires pour la réalisation de certaines opérations.

Pour pouvoir à nouveau accéder au dispositif Sécur'Pass, l'Abonné devra procéder à une nouvelle activation.

La suspension ou la fermeture de l'accès à Sécur'Pass pour quelque raison que ce soit, à l'initiative de l'Abonné ou de la Banque, entraîne l'impossibilité d'utiliser l'application Sécur'Pass et les fonctionnalités liées.

4.3 – Principes de sécurité

Le mot de passe et le Code d'authentification sont personnels et confidentiels et l'Abonné est responsable de leur usage et de leur conservation. En conséquence, la Banque ne peut être tenue pour responsable des dommages résultant d'un usage frauduleux ou abusif des dispositifs d'authentification.

L'Abonné prend toute mesure raisonnable pour préserver la sécurité de son identifiant, de son mot de passe, du Code et de tout élément d'authentification appartenant aux trois catégories ci-dessus. Il s'oblige à les tenir secrets et à ne les communiquer ou les remettre à quiconque.

En cas de perte, de vol, de divulgation ou de compromission de l'un quelconque des dispositifs d'authentification, l'Abonné s'engage à en informer immédiatement la Banque par tout moyen et à le lui confirmer par écrit dans les 24 heures, ou, le cas échéant, à modifier sans délai son Identifiant et/ou dispositif d'authentification depuis le Site. En cas d'utilisation de codes comme unique dispositif d'authentification, l'Abonné est invité à les modifier régulièrement depuis le Site, même en l'absence de perte ou de divulgation. De même, il est conseillé à l'Abonné de ne pas choisir un code confidentiel facilement décelable par un tiers (date de naissance par exemple). La saisie de trois codes erronés entraîne le blocage de l'accès au Service. Dans ce cas, le Service sera de nouveau accessible sur demande expresse formulée par l'Abonné auprès de la Banque.

4.4 – Accès au compte de paiement et initiation de paiement

Dès lors que l'Abonné autorise l'accès à son compte par un prestataire de service d'initiation de paiement ou d'information sur les comptes, ce prestataire doit disposer de l'agrément délivré par l'autorité compétente d'un Etat membre de l'Union Européenne ou être inscrit sur le registre tenu par cette autorité, conformément à la réglementation en vigueur. L'Abonné est tenu de vérifier que ce prestataire, à qui il communique ses identifiant et mot de passe, dispose de cet agrément ou est inscrit sur le registre concerné.

L'initiation d'opérations de paiement (virements) par ce prestataire, pour le compte de l'Abonné, s'effectuera selon les mêmes modalités et conditions d'authentification que si l'Abonné réalisait directement ces opérations par l'intermédiaire de Cyberplus.

ARTICLE 5 : SPÉCIFICITÉS DE CERTAINES FONCTIONNALITÉS

5.1 – Souscription aux services

L'Abonné peut souscrire dans le respect de la réglementation en vigueur applicable à certains services offerts par la Banque. La souscription effective du contrat ou la prise en compte d'un avenant peut être subordonnée au renvoi du contrat ou de l'avenant signé dans les délais qui seront indiqués à l'Abonné.

Dans le cadre de son abonnement à Cyberplus, l'Abonné peut accéder à certains services proposés par la Banque ou ses Partenaires, exclusivement par Cyberplus. L'accès effectif s'effectue après activation du service par ses soins et acceptation de Conditions Générales d'utilisation spécifiques, distinctes du présent contrat. L'Abonné peut également désactiver certains services par l'intermédiaire de Cyberplus. Cette désactivation vaut résiliation du contrat et du service concerné.

5.2 – Virements

L'Abonné peut effectuer des virements de l'un de ses comptes de dépôt ou d'épargne vers un autre de ses comptes de dépôt ou d'épargne et/ou des virements de l'un de ses comptes de dépôt vers un compte de dépôt de tiers ouvert à la Banque ou dans les livres de tout autre établissement de crédit, sous réserve d'avoir signé préalablement une convention de compte de dépôt et, le cas échéant, une convention de compte d'épargne auprès de la Banque.

Les caractéristiques des services de virements et les modalités d'exécution des virements sont décrites dans la convention de compte de dépôt, et, le cas échéant, de compte d'épargne, en vigueur.

Les opérations de virements sont traitées les jours ouvrables, pour la

Banque. Les virements reçus avant l'heure limite fixée actuellement à 17 heures seront traités à J (sous réserve de provision sur le compte à débiter). Au-delà, ils seront traités le jour ouvrable suivant. Si le moment de réception n'est pas un jour ouvrable pour la Banque, l'ordre de virement est réputé avoir été reçu le jour ouvrable suivant. Pour des raisons de sécurité, des plafonds sont appliqués par la Banque sur le montant des virements externes réalisés par l'intermédiaire du service CyberPlus. La Banque est également susceptible d'appliquer des mesures complémentaires visant à protéger l'Abonné de tout risque d'utilisation frauduleuse de son abonnement.

L'émission de virements vers un tiers nécessite que l'Abonné ajoute préalablement le compte du bénéficiaire sur une liste de bénéficiaires de virements. L'ajout de ce compte sur cette liste de bénéficiaires ainsi que l'émission d'un virement externe nécessitera l'authentification du client.

En revanche, l'émission d'un virement vers un compte dont l'Abonné est titulaire, ouvert dans les livres de la Banque, ne donnera pas lieu à cette authentification.

5.3 – Service d'agrégation de comptes (sous réserve de disponibilité)

Dans le cadre de son abonnement à Cyberplus, l'Abonné peut avoir accès à un service d'agrégation de comptes gratuit permettant notamment d'accéder à des fonctionnalités d'agrégation de comptes étendues. Ces fonctionnalités nécessitent l'acceptation préalable de Conditions Générales d'Utilisation distinctes.

La résiliation de l'abonnement à Cyberplus entraîne la fermeture du service d'agrégation de comptes.

5.4 – Catégorisation des dépenses et de revenus

Cette fonctionnalité permet de catégoriser automatiquement les opérations de l'Abonné enregistrées sur son compte (individuel ou joint). Les écritures catégorisées sont disponibles pendant une période de 26 mois glissants à partir de la date de l'opération. Les opérations sont classées dans diverses catégories (Alimentation, Logement...), permettant de disposer d'une meilleure lisibilité des dépenses et revenus. L'Abonné a la possibilité de modifier la catégorisation d'une opération. En cas de résiliation de l'abonnement à Cyberplus, l'ensemble des personnalisations et des catégorisations seront alors définitivement perdues.

5.5 – Localisation des commerçants auprès desquels le Client a effectué une opération de paiement :

Cette fonctionnalité permet au Client, qui consulte au moyen de Cyberplus le détail d'une opération de paiement qu'il a réalisé par carte bancaire, d'afficher sur un plan l'adresse du commerçant auprès duquel ladite opération a été effectuée. Cet affichage est réalisé sur la base des coordonnées GPS de l'adresse que le commerçant a préalablement déclarée, et est matérialisé par la visualisation d'un repère sur un plan généré par une application de cartographie (Google Maps, Plans) installée sur le matériel du Client et utilisant son adresse IP.

Dans ce cadre, le Client reconnaît avoir pris connaissance des conditions générales relatives à l'utilisation de l'application de cartographie qu'il utilise, disponibles auprès de Google ou Apple :

- Google Maps : <https://policies.google.com/privacy>

- Plans (Apple) : <https://www.apple.com/legal/privacy/>

Seules les opérations de paiement réalisées par carte bancaire chez des commerçants équipés de terminaux de paiement électroniques sont concernées par cette fonctionnalité, à l'exclusion des opérations réalisées à distance.

Le Client est informé que l'affichage de l'adresse du commerçant n'a qu'une valeur indicative, la Banque Populaire ne saurait être tenue pour responsable d'une erreur ou d'une absence de mise à jour de ses coordonnées GPS par le commerçant.

Par ailleurs, le Client peut à tout moment choisir de désactiver cette fonctionnalité dans les paramètres de Cyberplus.

5.6 – Fonctionnalités de pilotage de la carte

Dans le cadre de son abonnement à Cyberplus, l'Abonné détenteur d'une carte bancaire émise par la Banque peut avoir accès à des fonctionnalités de gestion en ligne de sa carte. Ces fonctionnalités sont décrites dans les Conditions générales de son Contrat Carte.

5.7 – Abonnement à des produits offrant des alertes sur la situation du compte par SMS

Dans le cadre de son abonnement à Cyberplus, l'Abonné dispose de la fonctionnalité lui permettant de recevoir des alertes par SMS

l'informant du solde de son compte et des opérations enregistrées sur celui-ci. L'Abonné peut paramétrer un mot clé, un montant, un type d'opération ou un franchissement de seuil, à la hausse ou à la baisse.

5.8 – Opérations sur instruments financiers et autres titres

Pour disposer de ce service, l'Abonné doit avoir préalablement signé une convention de compte d'instruments financiers auprès de la Banque. Les ordres saisis en dehors des horaires d'ouverture du marché seront présentés à la prochaine séance du marché concerné. Les passations d'ordres fermes s'effectuent sur la totalité des valeurs cotées sur les marchés financiers français hors MATIF, MONEP, marchés de matières premières et de marchandises.

ARTICLE 6 : RESPONSABILITÉS

6.1 – Responsabilité de la Banque

La Banque s'engage à tout mettre en œuvre pour assurer à l'Abonné le bon fonctionnement de CyberPlus, notamment la bonne exécution des ordres reçus et la confidentialité des informations communiquées. D'une manière générale, la Banque ne pourra être tenue pour responsable que des dommages ayant pour cause unique son propre fait.

Au cas où la responsabilité de la Banque serait établie, seul le préjudice personnel, prévisible, matériel et direct peut donner lieu à réparation.

La Banque ne saurait être tenue pour responsable :

- en cas de non-respect des procédures d'utilisation des services de CyberPlus ;

- en cas de divulgation d'un dispositif d'authentification à une tierce personne, y compris à un prestataire de service d'initiation de paiement ou d'information sur les comptes, disposant d'un agrément ou d'un enregistrement prévu par les textes en vigueur ;

- lorsque les informations communiquées lors de l'adhésion de l'Abonné ou lors de l'utilisation de CyberPlus s'avèrent inexactes ou incomplètes ;

- en cas d'interruption des prestations pour des raisons résultant de la force majeure, du cas fortuit ou du fait d'un tiers ;

- en cas de connexion de l'Abonné à un autre site que le site légitime et sécurisé de la Banque (<https://www.occitane.banquepopulaire.fr>).

La Banque n'est pas responsable du transport des données, de la qualité et de la disponibilité des réseaux de télécommunication, ni des interruptions pour les interventions de maintenance, par suite de cas fortuits ou de force majeure et, en particulier, celles qui se produisent suite à un mauvais fonctionnement du matériel de l'Abonné ou du réseau de télécommunications.

La Banque dégage sa responsabilité des difficultés associées au contrat passé entre l'Abonné et son fournisseur d'accès.

La Banque demeure étrangère à tout litige pouvant survenir entre l'Abonné et :

- tout prestataire substitué, tant en ce qui concerne la facturation des coûts des transmissions que le bon fonctionnement du réseau téléphonique ;

- le prestataire de services fournisseur d'accès Internet en ce qui concerne l'accès aux différents sites Internet ;

- le fournisseur du matériel informatique (modem, ordinateur, logiciels...) destiné à recevoir les informations par l'intermédiaire du téléchargement des écritures ;

- son prestataire de service d'initiation de paiement ou d'information sur les comptes.

La Banque n'est pas responsable des conséquences résultant d'un défaut de sécurité (matériel ou logiciel, antivirus) du terminal de connexion (ordinateur, terminal mobile...) utilisé par l'Abonné n'ayant pas détecté, notamment, l'intrusion d'un virus informatique.

De même, la responsabilité de la Banque ne saurait être engagée en raison des conséquences directes et indirectes liées aux mesures, quelles qu'elles soient, notamment de gel des avoirs, qu'elle pourrait être amenée à prendre dans le cadre des obligations mises à sa charge par les pouvoirs publics, en particulier au titre de la lutte contre le blanchiment des capitaux et le financement du terrorisme. À ce titre, la Banque ne saurait être tenue pour responsable des retards d'exécution.

La Banque se réserve le droit de limiter l'accès de l'Abonné aux seules fonctions de consultation ou de bloquer l'accès à CyberPlus, pour des raisons objectivement motivées liées à la sécurité du Service, à la présomption d'une utilisation non autorisée ou frauduleuse du service ou au risque sensiblement accru ou avéré que l'Abonné soit dans l'incapacité de s'acquitter de son obligation de

paiement. Dans ces cas, la Banque informe l'Abonné, par tout moyen, du blocage et des raisons de ce blocage, si possible avant que le Service ne soit bloqué ou immédiatement après sauf si cette information est impossible pour des raisons de sécurité ou interdite par une législation communautaire ou nationale. La Banque débloque le service dès lors que les raisons du blocage n'existent plus. La Banque met en place les moyens appropriés permettant à l'Abonné de demander à tout moment le déblocage du service.

La Banque informera l'Abonné par tout moyen, de façon sécurisée, en cas de soupçon de fraude, de fraude avérée ou de menaces pour la sécurité survenant sur le service de banque à distance.

6.2 – Responsabilité de l'Abonné

L'Abonné s'engage, notamment, au respect des conditions d'utilisation de CyberPlus et particulièrement au respect des instructions liées à la sécurité du service.

L'Abonné est responsable de la protection de son terminal de connexion (ordinateur, terminal mobile...) notamment au travers de tout moyen permettant de lutter contre l'intrusion d'un virus informatique.

L'Abonné est tenu de sécuriser son ordinateur, sa tablette ou son téléphone mobile au moyen de solutions de sécurité de son choix (verrouillage du téléphone, logiciel anti-virus et anti-espion, pare-feu, logiciels de nettoyage...) et de maintenir ces dispositifs à jour en permanence. Il est conseillé à l'Abonné d'utiliser un téléphone mobile fonctionnant avec Android ou IOS et déconseillé d'utiliser les autres types de systèmes d'exploitation. Il lui est interdit de procéder au déverrouillage des systèmes d'exploitation.

L'Abonné est ainsi invité à prendre connaissance des mesures à mettre en œuvre afin de sécuriser ses connexions Internet en consultant les informations relatives à la sécurité disponibles sur le Site.

Dans le souci de protéger la confidentialité des données bancaires de l'Abonné, la Banque, en particulier dans le cadre des règles d'usage d'Internet, invite celui-ci à prendre toutes les dispositions utiles, notamment en effaçant, dès la fin de sa consultation, les traces de sa navigation et en interdisant l'accès aux tiers non autorisés dans l'hypothèse du téléchargement de ces données bancaires vers un logiciel de gestion.

Conformément aux articles L.133-19 et L.133-20 du code monétaire et financier, lorsque les opérations de paiement non autorisées sont effectuées par l'intermédiaire des services de banque à distance, suite à la perte, au vol, au détournement ou à toute utilisation non autorisée de ce service ou des données qui lui sont liées, les règles spécifiques suivantes s'appliquent.

Avant la demande de blocage de l'instrument (appelé aussi mise en opposition) :

- l'Abonné supporte les pertes financières à hauteur de 50 euros en cas d'opération de paiement non autorisée consécutive à la perte ou au vol de ses dispositifs d'authentification et effectuée en utilisant les services de banque à distance pour l'émission d'ordres de virement en ligne ;

- l'Abonné ne supporte aucune conséquence financière en cas :

- de perte ou de vol des données de sécurité personnalisées ne pouvant être détecté par l'Abonné avant le paiement de l'Abonné,
- de perte de ces données due à des actes ou à une carence d'un salarié, agent ou d'une succursale de la Banque ou d'une entité vers laquelle ses activités ont été externalisées.

La responsabilité de l'Abonné n'est pas engagée non plus lorsque l'opération non autorisée a été effectuée en détournant, à l'insu de l'Abonné, les données liées à l'instrument de paiement et en cas de contrefaçon de l'instrument.

Si la banque du bénéficiaire n'est pas située dans l'Espace Economique Européen, l'Abonné supporte les pertes liées à l'utilisation de ses données de sécurité personnalisées avant l'information relative à la perte ou au vol dans la limite d'un plafond de 50 €

Après la demande de blocage de l'instrument (appelé aussi mise en opposition), l'Abonné ne supporte aucune conséquence financière.

De façon générale, les opérations non autorisées sont à la charge de l'Abonné en cas d'agissements frauduleux de sa part ou s'il n'a pas satisfait intentionnellement ou par négligence grave à son obligation générale de prudence rappelée dans la convention de compte en vigueur.

Sauf agissement frauduleux de sa part, l'Abonné ne supporte aucune conséquence financière si l'opération de paiement non autorisée a été effectuée sans que la Banque n'exige une authentification forte du Client dans le respect de la procédure

d'authentification forte mise en place par la Banque.

En particulier, la responsabilité de l'Abonné est engagée en cas de manquement à ses obligations de :

- prendre toute mesure pour conserver ses dispositifs d'authentification, préserver leur sécurité et leur confidentialité,
- demander sans tarder le blocage de l'instrument, dès qu'il a connaissance de la perte, du vol, du détournement ou de toute utilisation non autorisée de cet instrument ou des données qui lui sont liées.

ARTICLE 7 : INFORMATIONS DIVERSES

L'Abonné reconnaît que les informations bancaires ou renseignements généraux ne concernant pas directement le fonctionnement de son ou ses comptes, présentent un caractère purement indicatif et ne peuvent, à ce titre, engager la responsabilité de la Banque.

Seuls les extraits de compte adressés par la Banque continuent de faire foi.

La transmission des données ayant lieu par Internet, environnement international ouvert et non sécurisé, la Banque ne saurait être responsable de l'utilisation, de la sécurité, de la conservation, de la confidentialité ou de l'intégrité des données transmises. Le téléchargement de données est donc réalisé sous l'entière responsabilité de l'Abonné.

Le Service peut renvoyer l'Abonné vers d'autres sites tiers dont la Banque n'est nullement propriétaire. En conséquence, la Banque ne saurait être tenue pour responsable du contenu de ces sites.

ARTICLE 8 : RÈGLES DE PREUVE

De convention expresse, toutes les connexions et opérations effectuées au moyen de l'Identifiant et du dispositif d'authentification de l'Abonné sont réputées avoir été effectuées par l'Abonné et équivalent à sa signature.

L'Abonné accepte l'enregistrement informatique des connexions et opérations réalisées au cours de l'utilisation du Service. Les parties consentent expressément à ce que le fichier des connexions et opérations initiées par l'Abonné fasse preuve entre les parties et ce, quel que soit le support matériel utilisé pour ces enregistrements. Ces fichiers auront la même valeur qu'un document original et feront foi en cas de contestation, sauf preuve contraire.

ARTICLE 9 : TARIFICATION DU SERVICE

Les fonctionnalités du service Cyberplus pourront être mises à disposition de l'Abonné gratuitement par la Banque ou moyennant le paiement d'un abonnement mensuel figurant dans les conditions tarifaires de la Banque en vigueur.

Le service CyberPlus peut également donner accès à de nouvelles fonctionnalités pouvant faire l'objet d'une facturation. Le montant de cette tarification est mentionné dans les conditions tarifaires en vigueur. Le coût des consommations téléphoniques entre le poste de l'Abonné et le serveur Internet reste à la charge de l'Abonné, ainsi que tout montant, redevance, abonnement ou taxe afférents à son abonnement téléphonique.

ARTICLE 10 : MODIFICATION DES CONDITIONS GENERALES ET LES CONDITIONS TARIFAIRES

10.1 – Modifications à l'initiative de la Banque

La Banque aura la faculté de modifier les Conditions Générales et les Conditions Tarifaires de ses services. À cet effet, la Banque communiquera à l'Abonné, au plus tard deux mois avant la date d'application envisagée, sur support papier ou sur tout autre support durable (par exemple, lettre, mention sur le relevé de compte ou information dans son espace personnel de banque à distance), le projet de modification.

La Banque et l'Abonné conviennent que l'absence de contestation de l'Abonné dans ce délai vaut acceptation par ce dernier des modifications. En cas de refus de l'Abonné, il peut résilier sans frais, avant la date d'application des modifications, le présent contrat et le service CyberPlus. À défaut de résiliation dans ce délai, les modifications lui seront opposables.

10.2 – Modifications imposées par des textes législatifs ou réglementaires.

Les modifications de tout ou partie des Conditions Générales, qui seraient rendues nécessaires par des dispositions législatives ou

réglementaires, seront applicables dès la date d'entrée en vigueur de celles-ci.

ARTICLE 11 : DURÉE DE L'ABONNEMENT – RÉSILIATION OU SUSPENSION

L'abonnement au service CyberPlus est conclu pour une durée indéterminée. Il pourra être résilié à tout moment par l'une ou l'autre des parties, par lettre recommandée avec avis de réception. Cette résiliation prendra effet dans le mois suivant la réception, par la Banque, du courrier recommandé envoyé par l'Abonné. La cotisation du mois en cours devra être payée par l'Abonné.

La résiliation par la Banque doit respecter un préavis de deux mois.

La résiliation de l'abonnement à CyberPlus entraîne la désactivation de l'ensemble des fonctionnalités et services de banque à distance activés à partir de CyberPlus.

En tout état de cause, pour l'Abonné ayant bénéficié du service « e-Documents », l'accès à l'espace de banque en ligne est maintenu même après la clôture du dernier contrat de l'Abonné, afin de permettre l'accès à l'historique des documents numériques dans les conditions spécifiques au service « e-Documents ».

La Banque pourra également suspendre l'accès ou l'exécution de tout ou partie des fonctionnalités de CyberPlus ou résilier la Convention, sans préavis ni formalité, pour motif grave et notamment en cas de tentative ou d'utilisation frauduleuse ou abusive du service par l'Abonné, ou en cas de rupture des relations commerciales (non-paiement d'une facture, clôture du compte...), ce dont l'Abonné en serait immédiatement informé.

Tout ordre donné avant la date de résiliation est exécuté aux conditions et dates convenues.

Le service CyberPlus pourra également être temporairement interrompu pendant des périodes courtes pour des raisons techniques et en vue de réaliser des prestations de maintenance ou d'actualisation du service CyberPlus ou de l'application mobile.

ARTICLE 12 : PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

Dans le cadre de la signature et de l'exécution des Conditions Générales et Particulières du service Cyberplus, et plus généralement de sa relation avec l'Abonné, la Banque en tant que responsable de traitement recueille et traite des données à caractère personnel concernant :

- l'Abonné et

- les personnes physiques intervenant dans le cadre de cette relation (mandataire, représentant légal, caution, contact désigné, préposé, bénéficiaire effectif, membre de la famille de l'Abonné...).

La Banque met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer que les traitements de données à caractère personnel sont effectués conformément à la réglementation applicable.

L'Abonné peut à tout moment et dans les conditions prévues par la réglementation, accéder aux informations le concernant, les faire rectifier, demander leur effacement, leur limitation, leur portabilité, ou communiquer des instructions sur leur sort en cas de décès.

Si le traitement lié à une fonctionnalité du Service est fondé sur l'intérêt légitime de la Banque (ex : la catégorisation des dépenses prévue pour la gestion de budget), l'Abonné peut à tout moment s'opposer à ce traitement s'il justifie de raisons propres à sa situation particulière et selon les modalités prévues dans la Notice d'information sur le traitement des données à caractère personnel.

De plus amples informations expliquant à l'Abonné pourquoi et comment ces données sont utilisées, combien de temps elles seront

conservées ainsi que les droits dont il dispose sur ses données figurent dans la Notice d'information sur le traitement des données à caractère personnel de la Banque.

Cette notice est portée à la connaissance de l'Abonné lors de la première collecte de ses données. Il peut y accéder à tout moment, sur le site internet de la Banque via l'adresse suivante : <https://www.occitane.banquepopulaire.fr/> ou en obtenir un exemplaire auprès de votre Agence.

La BANQUE POPULAIRE OCCITANE communiquera en temps utile les évolutions apportées à ces informations.

ARTICLE 13 : RÉCLAMATIONS - MÉDIATION

En cas de difficultés concernant ces produits et services, l'Abonné peut obtenir de son agence toutes les informations souhaitées, formuler auprès d'elle toute réclamation et, en cas de difficultés persistantes, saisir par écrit le « Service Relations Clients » de la Banque qui s'efforce de trouver avec lui une solution.

La saisine du « Service Relations Clients » de la Banque est effectuée par lettre envoyée à l'adresse suivante :

« BANQUE POPULAIRE OCCITANE, Service Relations Clients, Camp La Courbisie, Avenue Maryse Bastié, B.P.19, 46022 CAHORS CEDEX. »

Tout renseignement relatif à une contestation peut être obtenu en téléphonant au numéro suivant : 05 81 22 00 00 (numéro non surtaxé).

La Banque s'engage à répondre à l'Abonné sous dix jours ouvrables.

Toutefois si une analyse plus approfondie de son dossier est nécessaire et entraîne un dépassement de délai, la Banque s'engage à lui communiquer le nouveau délai qui, sauf cas très particulier ne devrait pas dépasser deux mois (à compter de la date de réception de sa réclamation). Concernant les réclamations liées aux services de paiement, une réponse sera apportée à l'Abonné dans les quinze jours ouvrables suivant la réception de sa réclamation. Cependant, si un délai supplémentaire est nécessaire pour lui répondre, la Banque lui adressera une réponse d'attente motivant ce délai et précisant la date ultime de sa réponse. En tout état de cause, l'Abonné recevra une réponse définitive au plus tard trente-cinq jours ouvrables suivant la réception de sa réclamation.

À défaut de solution le satisfaisant ou en l'absence de réponse dans ces délais, l'Abonné a la faculté de saisir gratuitement le médiateur de la Banque sur son site internet ou par voie postale, dans le délai d'un an à compter de sa réclamation auprès de la Banque, sans préjudice des autres voies d'actions légales dont il dispose.

L'adresse postale du médiateur et les coordonnées du site internet du médiateur figurent sur les brochures tarifaires et le site internet de la Banque.

Les informations nécessaires à la saisine du médiateur, son périmètre et le déroulé de la procédure de médiation figurent sur la charte de médiation disponible sur le site internet du médiateur <https://www.mediateur-fnbp.fr/>.

En cas de souscription par internet, l'Abonné peut également déposer sa réclamation sur la plateforme européenne de règlement par voie extrajudiciaire des litiges en ligne qui orientera sa demande : <http://ec.europa.eu/consumers/odr/>.

ARTICLE 14 : LOI APPLICABLE – COMPÉTENCE - LITIGES

Le présent contrat est conclu en langue française. L'Abonné accepte expressément l'usage de la langue française durant les relations précontractuelles et contractuelles. La Convention est soumise à la loi française et à la compétence des tribunaux français.