

CONDITIONS PARTICULIERES DE L'APPLICATION BANCAIRE



Table des matières

I.	Services de l'Application bancaire.....	3
II.	Sécurité.....	3
III.	Responsabilité	4
IV.	Suspension de l'Application bancaire	5
V.	Charges	5
VI.	Modification des conditions particulières.....	5
VII.	Helpdesk.....	5

Outre l'application des Conditions Générales, les présentes conditions particulières régissent les droits, obligations et responsabilités particulières qu'entraîne l'utilisation de l'Application bancaire (les **Conditions Particulières de l'Application bancaire**).

En cas de contradiction avec les Conditions Générales, les Conditions Particulières de l'Application Bancaire prévalent sur les Conditions Générales.

Toutes les conditions sont toujours disponibles gratuitement en français, en néerlandais et en anglais sur www.medirect.be.

I. Services de l'Application bancaire

Le Client peut utiliser l'Application bancaire pour effectuer les Services suivants :

- à des fins d'authentification («Soft token») pour accéder au Site internet dédié ;
- consulter et gérer tous ses Comptes ;
- effectuer des virements bancaires à des tiers et transférer de l'argent entre ses Comptes ;
- lire et envoyer des Notifications ; et
- exécuter tout autre Service supplémentaire que la Banque pourrait fournir par suite d'une mise à jour de l'Application bancaire.

Toute utilisation de l'Application bancaire à d'autres fins est interdite.

Toute reproduction, copie, modification, adaptation, falsification et/ou rétro-ingénierie de tout ou partie de l'Application bancaire est interdite.

II. Sécurité

L'utilisation par le Client de l'Application bancaire est soumise à toutes les exigences de sécurité énoncées dans les Conditions Particulières de l'Application bancaire, y compris son obligation de protéger son appareil mobile et ses transmissions contre tout accès non autorisé.

Le Client doit prendre toutes les mesures raisonnables pour garantir la sécurité et l'intégrité de l'Application bancaire.

Par conséquent :

- le Client s'abstient de laisser l'Application bancaire sans surveillance ;
- le Client ne confie jamais l'Application bancaire et ses moyens d'accès et de signature à des tiers et n'autorise jamais personne à en faire usage ;
- le Client ne communique jamais ses moyens d'authentification et ne les note jamais sur papier ou sur tout autre support durable ;
- le Client introduit discrètement ses moyens d'authentification et veille à ce que personne ne puisse les distinguer ;
- lorsqu'il choisit un nouveau mot de passe ou code PIN, le client évite les combinaisons évidentes et qui peuvent facilement être piratées.

Il est demandé au Client de suivre au moins les étapes suivantes pour éviter tout accès frauduleux à l'Application bancaire et aux Services associés :

- changer immédiatement le mot de passe et appeler immédiatement le service clientèle de la Banque (voir ci-dessous) en cas de soupçon de prise de connaissance par un tiers du mot de passe ;
- ne pas télécharger ni installer de programme ou d'application de source inconnue ;
- ne pas utiliser de Wi-Fi public ;
- prendre toutes les précautions raisonnables et adéquates pour protéger son appareil de tout virus ou autre propriété destructive.

Le Client contacte le service clientèle de la Banque au +32 (0)2 887 20 05, qui est accessible pendant les heures de bureau (du lundi au vendredi de 9h à 20h et le samedi de 9h à 14h). En dehors des heures de bureau (du lundi au vendredi de 20h à 9h, le samedi de 14h à minuit et les dimanches et jours fériés 24h/24), le Client contacte le service de permanence de la Banque au +32 (0)2 887 20 04.

Le Client est tenu d'informer la Banque immédiatement s'il soupçonne une mauvaise utilisation de son appareil. Il sera tenu responsable de toute perte réelle de fonds ou de toute interception d'informations par un accès non autorisé à son appareil dans l'éventualité où il a contribué à cet accès non autorisé par fraude, négligence ou en divulguant volontairement son code d'accès à quiconque, y compris un membre de sa famille ou un ami.

Le Client ne doit pas utiliser l'Application bancaire sur un appareil ou un système d'exploitation qui a été modifié en dehors des configurations prises en charge ou garanties par l'appareil mobile ou par le fournisseur du système d'exploitation. Cela inclut les appareils qui ont été « débridés (jail-broken) » ou « rooted ».

La Banque s'engage à fournir au client les moyens nécessaires pour signaler à tout moment l'utilisation abusive de l'Application bancaire et pour prouver qu'il a bien effectué un tel signalement, à empêcher, dans la mesure des possibilités techniques, tout nouvel usage de l'Application bancaire aussitôt que le client en a signalé la perte, le vol ou l'utilisation abusive, à informer périodiquement le client sur les mesures de prévention à prendre pour empêcher tout usage illicite de l'Application Bancaire et à l'informer de toute fraude suspectée ou avérée, ainsi que des menaces pour la sécurité.

Toute communication à adresser spécifiquement au client en cas de fraude suspectée ou avérée sur l'Application bancaire est effectuée par téléphone ou par courriel.

La Banque et ses fournisseurs de Services utiliseront les informations fournies par le Client dans le but de fournir les Services et de préparer des analyses et compilations de données Clients « agrégées ». Ces données n'identifient pas personnellement le Client, mais se contentent de données générales (par exemple le nombre de Clients qui se sont inscrits en un mois). Si le Client utilise les Services de l'Application bancaire, la Banque peut recueillir et traiter les données personnelles du Client en fonction de son emplacement réel, tel que les signaux GPS envoyés par un appareil mobile. La Banque recueille et traite toutes les données personnelles du Client conformément à sa politique de confidentialité, qui est disponible sur

<https://www.medirect.be/wp-content/uploads/Privacy-policy-fr-1.pdf>.

En acceptant les Conditions Générales, le Client confirme qu'il accepte les conditions de notre politique de confidentialité et de traitement des données.

III. Responsabilité

La Banque ne saurait être tenue responsable de tout manquement à fournir les Services de l'Application bancaire, en tout ou en partie, en raison de circonstances imprévues ou indépendantes de sa volonté.

La Banque n'est pas responsable de toute perte monétaire causée lorsque :

- le Client ne peut pas accéder à l'Application bancaire pour quelque raison que ce soit ou que celle-ci est lente à répondre;
- l'appareil, le matériel ou le logiciel utilisé par le Client pour accéder à l'Application bancaire est endommagé, corrompu, perdu, volé ou ne fonctionne pas ;
- l'Application bancaire ne fonctionne pas comme le Client s'y attend, ne répond pas à ses exigences, n'est pas adaptée à l'usage auquel il l'a destinée ou contient des erreurs ou des défauts ;
- le Client ne reçoit pas un SMS ou un message dans l'Application bancaire à temps ;
- la Banque est empêchée de fournir un Service en tout ou en partie à cause d'un acte commis par une tierce partie ; ou
- le Client néglige de mettre à jour l'Application bancaire.

Apple Inc., Google Inc. et Microsoft Corporation n'assument aucune responsabilité ou obligation envers le Client en ce qui concerne l'Application bancaire et ne fournissent aucun service de maintenance et de support pour l'Application bancaire.

L'Application bancaire est fournie "telle quelle", sans aucune représentation, garantie ou accord de quelque nature que ce soit quant à sa fonctionnalité. La Banque ne peut pas garantir qu'aucun virus ou autre propriété contaminante ou destructrice ne sera transmis ou qu'aucun dommage ne sera causé à l'appareil, au matériel ou au logiciel du Client.

Le Client est requis d'aviser immédiatement la Banque de la perte, du vol, de la mauvaise utilisation ou du risque de mauvaise utilisation des mots de passe, codes PIN, cartes ou appareils le cas échéant.

IV. Suspension de l'Application bancaire

La Banque peut annuler ou suspendre l'accès du Client et son utilisation de l'Application bancaire sans préavis (sauf interdiction légale) quand :

- la Banque a des raisons de soupçonner que le Client est engagé dans un comportement frauduleux ou inapproprié ;
- tous les Comptes du Client ont été fermés ;
- le système ou l'équipement de la Banque ne fonctionne pas correctement ou n'est pas disponible pour l'utilisation ;
- la Banque estime que la sécurité de l'accès du Client ou du système et de l'équipement de la Banque peut avoir été compromise ; ou
- la Banque est tenue de le faire conformément à la loi.

Le cas échéant, la Banque donnera au Client un préavis dans un délai raisonnable. Dans certains cas, il est possible que la Banque ne soit pas en mesure de donner un préavis au Client en raison d'obligations légales. Si ce dernier a saisi plusieurs fois des données de connexion erronées sur l'Application de signature électronique, la Banque peut suspendre son accès à l'Application bancaire et au Site internet dédié.

V. Charges

Le téléchargement, l'enregistrement et l'utilisation de l'Application bancaire sont gratuits.

Des frais peuvent être appliqués par le fournisseur de réseau mobile du Client. La Banque ne sera pas responsable de ces frais.

VI. Modification des Conditions Particulières de l'Application bancaire

La Banque peut modifier ou compléter à sa seule discrétion les Conditions Particulières de l'Application bancaire en suivant les dispositions de l'article I.15 des Conditions Générales.

VII. Helpdesk

Service clientèle de MeDirect (par e-mail à complaints@medirect.be, par téléphone au +32 (0) 2 887 20 05 ou via un autre moyen de communication sécurisé).