Conditions pour les services de banque en ligne

Utilisation de l'application ou des interfaces utilisateur du partenaire de Solarisbank

Outre les Conditions Générales de la Banque, les conditions particulières suivantes (ci-après : les Conditions) s'appliquent à l'utilisation du service de banque en ligne mis à disposition par Solarisbank AG (ci-après : la "Banque") au moyen de l'application ou de l'interface utilisateur par navigateur du partenaire de Solarisbank (ci-après : l'"Interface Utilisateur").

1. Gamme de services

(1) Le client ou son représentant autorisé peut effectuer des opérations bancaires par le biais des services de banque en ligne dans la mesure où le Banque le propose. Ils peuvent également accéder aux informations de la Banque par le biais des services de banque en ligne. En outre, ils sont autorisés à utiliser les services d'initiation de paiement et les services d'information sur les comptes tels que définis par le Code monétaire et financier. En outre, ils peuvent utiliser d'autres services tiers qu'ils ont sélectionnés.

(2) Les clients et les représentants autorisés sont uniformément désignés par le terme "Participants", les comptes et dépôts par le terme "Compte", sauf indication contraire explicite.

(3) Les limites de transaction convenues séparément avec la Banque s'appliquent à l'utilisation des services de banque en ligne.

2. Conditions d'utilisation de la banque en ligne

(1) Le Participant peut utiliser les services de banque en ligne si la Banque l'a authentifié.

(2) L'authentification est la procédure convenue séparément avec la Banque, par laquelle la Banque peut vérifier l'identité du Participant ou l'utilisation autorisée d'un instrument de paiement convenu, y compris l'utilisation du dispositif de sécurité personnalisé du Participant. En utilisant les éléments d'authentification convenus à cet effet, le Participant peut s'identifier auprès de la Banque en tant que Participant autorisé, accéder aux informations (voir Article 3 des présentes Conditions) et passer des ordres (voir Article 4 des présentes Conditions).

(3) Les éléments d'authentification sont

- les éléments de connaissance, c'est-à-dire quelque chose que seul le participant connaît (par exemple, le numéro d'identification personnel (NIP)),
- des éléments de possession, c'est-à-dire quelque chose que seul le participant possède (par exemple, un appareil permettant de générer ou de recevoir des numéros de transaction uniques (TAN) qui prouvent la propriété de l'abonné, comme la carte « girocard » avec générateur de TAN ou le terminal mobile), ou
- des éléments d'inhérence, c'est-à-dire quelque chose que le Participant est (par exemple les empreintes digitales comme caractéristique biométrique du Participant).

(4) La Banque authentifie le Participant sur la base de la transmission par celui-ci de l'élément de connaissance, de la preuve de l'élément de possession et/ou de la preuve de l'élément d'existence à la Banque conformément à la demande de celle-ci.

3. Accès aux services de banque en ligne

Le Participant a accès aux services de banque en ligne lorsque

- il saisit son numéro de client individuel (par exemple, son numéro de compte, son nom de connexion) et
- il s'identifie à l'aide du (des éléments d'authentification demandés par la Banque, et
- l'accès n'est pas bloqué (voir les Articles 8.1 et 9 des présentes Conditions).

Une fois l'accès à la banque en ligne accordé, les informations peuvent être consultées ou les commandes peuvent être passées conformément à l'Article 4 des présentes Conditions.

(2) Pour l'accès aux données de paiement sensibles, à savoir les données pouvant être utilisées pour commettre des transactions frauduleuses, (par exemple pour le changement d'adresse du client), la Banque demande au participant de s'identifier en utilisant un élément d'authentification supplémentaire si un seul élément d'authentification a été demandé pour l'accès aux services de banque en ligne. Le nom du titulaire du compte et le numéro de compte ne sont pas considérés comme des données de paiement sensibles pour les services d'initiation de paiement et les services d'information sur les comptes utilisés par le participant.

4. Ordres

4.1 Emission d'ordres

Le Participant doit accepter un ordre (par exemple un virement bancaire) pour qu'il soit valide (autorisation). Sur demande, le Participant doit utiliser des éléments d'authentification (par exemple, en saisissant un TAN comme preuve de propriété).

La Banque confirme la réception de la commande par le biais des services de banque en ligne.

4.2 Annulation des ordres

Les hypothèses et modalités dans lesquelles un ordre passé par la banque en ligne peut être annulé sont régies par les conditions spéciales qui s'appliquent au type d'ordre concerné (conditions pour les virements, par exemple). Les ordres ne peuvent être annulés qu'en dehors des services de banque en

ligne, à moins que la Banque n'ait expressément prévu une option d'annulation dans ses services de banque en ligne.

5. Traitement des ordres par la Banque

(1) Les ordres sont traités les jours ouvrables indiqués pour le traitement du type d'ordre en question (un virement, par exemple) sur la page de la banque en ligne ou dans la « Liste des Prix et des Services », dans le cadre du déroulement normal des opérations. Si l'ordre est reçu après l'heure indiquée sur la page de la banque en ligne de la Banque ou dans la « Liste des Prix et des Services » (délai d'acceptation) ou si l'heure de réception ne tombe pas un jour ouvré tel que défini par la « Liste des Prix et des Services » de la Banque, l'ordre est réputé avoir été reçu le jour ouvré suivant. Le traitement ne commence que ce jour-là.

(2) La Banque exécute l'ordre si les conditions d'exécution suivantes sont remplies :

- Le Participant a autorisé l'ordre (cf. Article 4.1 des présentes Conditions).
- Le participant est autorisé à effectuer le type de transaction concerné (une opération sur titres, par exemple).
- Le format des données bancaires en ligne est respecté.
- La limite des opérations bancaires en ligne convenue séparément n'est pas dépassée.
- Les exigences supplémentaires pour l'exécution du type d'ordre concerné sont respectées conformément aux conditions spéciales pertinentes (fonds suffisants sur le compte pour le transfert, par exemple).

Si ces conditions d'exécution sont réunies, la Banque exécute les ordres conformément aux dispositions des conditions spéciales applicables au type d'ordre concerné (conditions de transfert, par exemple, ou conditions de l'opération sur titres).

(3) Si les conditions d'exécution visées au paragraphe 2ne sont pas réunies, la Banque ne peut pas exécuter l'ordre. La Banque en informe le Participant par le biais des services de banque en ligne et lui explique ainsi, dans la mesure du possible, les raisons de cette situation et les moyens de corriger les erreurs qui ont conduit au refus de l'ordre par le biais des services de banque en ligne. Cela ne s'applique pas lorsque le fait de donner des raisons enfreint d'autres dispositions de la loi.

6. Informations fournies au client sur les opérations bancaires en ligne

La Banque informe le client au moins une fois par mois des opérations effectuées par les services de banque en ligne selon la méthode convenue pour la fourniture des informations sur les comptes.

7. Devoir de diligence du Participant

7.1 Protection des éléments d'authentification

(1) Le Participant prend toutes les précautions raisonnables pour protéger ses éléments d'authentification (voir Article 2 des présentes Conditions) contre tout accès non autorisé. Dans le cas contraire, il existe un risque d'abus ou d'utilisation non autorisée des services de banque en ligne (cf. Articles 3 et 4 des présentes Conditions).

(2) Afin de protéger les différents éléments d'authentification, le Participant accorde une attention particulière aux points suivants :

a) Les éléments de connaissance, tels que le code PIN, sont tenus secrets ; en particulier, ils ne peuvent pas :

- être communiqués oralement (notamment par téléphone ou en personne),
- être transmis sous forme de texte en dehors des services de banque en ligne (par exemple par courrier électronique, service de messagerie),
- être stockés de manière non sécurisée par voie électronique (par exemple, stockage du code PIN en texte clair sur un ordinateur ou un appareil mobile) et
- être enregistrés sur un appareil ou stocké sous forme de transcription avec un appareil qui sert d'élément de possession (par exemple, carte d'authentification avec générateur de TAN, terminal mobile, carte de signature) ou de vérification de l'élément d'inhérence (par exemple, terminal mobile avec application pour la banque en ligne et capteur d'empreintes digitales).

b) Les éléments de possession tels que la carte d'authentification avec générateur de TAN ou un terminal mobile doivent être protégés contre les abus, en particulier :

- la carte bancaire avec générateur de TAN ou la carte de signature doit être protégée contre tout accès non autorisé par d'autres personnes,
- il faut s'assurer que les personnes non autorisées ne peuvent pas accéder au terminal mobile du Participant (par exemple, un téléphone portable),
- il faut veiller à ce que d'autres personnes ne puissent pas utiliser l'application sur l'appareil mobile (par exemple, le téléphone portable) pour les opérations bancaires en ligne (par exemple, l'application de banque en ligne, l'application d'authentification),
- l'application liée aux services de banque en ligne (par exemple, application de banque en ligne, application d'authentification) sur le terminal mobile du Participant doit être désactivée avant que le Participant ne cède ce terminal mobile (par exemple, en vendant ou en donnant le téléphone mobile),

- la preuve de l'élément de propriété (par exemple, le TAN) ne peut être transmise oralement (par exemple, par téléphone) ou sous forme de texte (par exemple, par courrier électronique, par service de messagerie) en dehors des services de banque en ligne, et
- le participant qui a reçu de la Banque un code pour activer l'élément de possession (par exemple, un téléphone portable avec une application pour les services de banque en ligne) doit le protéger contre tout accès non autorisé par d'autres personnes ; sinon, il y a un risque que d'autres personnes activent leur appareil comme élément de possession pour l'utilisation des services de banque en ligne du participant.

c) Les éléments d'inhérence, tels que l'empreinte digitale du Participant, ne peuvent être utilisés comme élément d'authentification pour les opérations bancaires en ligne sur le terminal mobile d'un Participant que si aucun élément d'inhérence d'une autre personne n'est stocké sur le terminal mobile. Si le terminal mobile utilisé pour les opérations bancaires en ligne stocke les éléments d'inhérence d'autres personnes, l'élément de connaissance délivré par la Banque (par exemple le code PIN) doit être utilisé pour les opérations bancaires en ligne et non l'élément d'inhérence stocké sur le terminal mobile.

(3) Le numéro de téléphone enregistré pour la procédure mobile de TAN est supprimé ou modifié si l'abonné n'utilise plus ce numéro de téléphone pour les opérations bancaires en ligne.

(4) Nonobstant les obligations de protection prévues aux paragraphes 1 à 4, le Participant peut utiliser ses éléments d'authentification vis-à-vis d'un service d'initiation de paiement et d'un service d'information sur les comptes de son choix ainsi que de tout autre service tiers (voir Article 1 paragraphe 1 phrases 3 et 4 des présentes Conditions). Les autres services de tiers sont sélectionnés par le Participant avec le plus grand soin.

7.2 Consigne de sécurité

Le Participant respecte les consignes de sécurité du site Internet de la Banque pour les services de banque en ligne, en particulier les mesures de protection du matériel et des logiciels utilisés (système client).

7.3 Vérification des données relatives aux ordres par rapport aux données affichées par la Banque

La Banque affiche au Participant les données de l'ordre qu'elle a reçues (par exemple le montant, le numéro de compte du bénéficiaire, le numéro d'identification des titres) via l'appareil convenu séparément du Participant (par exemple un terminal mobile, un lecteur de carte à puce avec écran). Le Participant est tenu, avant la confirmation, de vérifier si les données affichées correspondent aux données spécifiées pour l'ordre.

8. Obligations d'information et de notification

8.1 Avis de blocage

(1) Si le participant a connaissance

- de la perte ou le vol d'un élément d'authentification,
- de l'utilisation abusive ou toute autre utilisation non autorisée d'un de ses éléments d'authentification ou d'un de ses dispositifs de sécurité personnels,

le Participant doit en informer la Banque sans délai (avis de blocage).

Le Participant peut à tout moment soumettre un avis de blocage à la Banque également via les coordonnées fournies séparément.

(2) Le Participant doit signaler immédiatement à la police tout vol ou usage abusif d'un élément d'authentification.

(3) Si le Participant soupçonne une utilisation non autorisée ou frauduleuse de l'un de ses éléments d'authentification, il doit également soumettre un avis de blocage.

8.2 Notification des ordres non autorisés ou incorrects

Le client doit signaler à la Banque tout ordre non autorisé ou incorrect dès qu'il le détecte.

9. Blocage de l'utilisation

9.1 Blocage à l'initiative du Participant

À la demande du Participant, notamment en cas de notification de blocage conformément à l'Article 8.1, la Banque impose un blocage

- sur l'accès aux services de banque en ligne pour lui ou tous les Participants ou
- de ses éléments d'authentification pour l'utilisation des services de banque en ligne.

9.2 Blocage à l'initiative de la Banque

(1) La Banque peut bloquer l'accès aux services de banque en ligne pour un Participant si

- elle est autorisée à résilier le contrat de banque en ligne pour un motif valable,
- des raisons matérielles relatives à la sécurité des éléments d'authentification le justifient ou
- elle suspecte une utilisation non autorisée ou frauduleuse de l'un des éléments d'authentification.

(2) La Banque informe le client du blocage, en précisant les raisons correspondantes, si possible avant le blocage, mais au plus tard immédiatement après le blocage. La Banque ne peut pas donner de raisons si cela constituerait un non-respect d'obligations légales.

9.3 Levée du blocage

La Banque lève le blocage ou remplace les éléments d'authentification pertinents si les raisons du blocage n'existent plus. Elle en informe immédiatement le client.

9.4 Blocage automatique d'un élément de possession à puce

(1) La carte à puce avec fonction de signature est automatiquement bloquée si le code à utiliser pour la signature électronique est erroné trois fois de suite.

(2) Un générateur de TAN faisant partie d'une carte à puce qui nécessite la saisie de son propre code d'utilisation se bloque s'il est erroné trois fois de suite.

(3) Les éléments de possession visés aux paragraphes 1 et 2 ne peuvent alors plus être utilisés pour les services de banque en ligne. Le Participant peut contacter la Banque afin de rétablir l'utilisation des services de banque en ligne.

9.5 Blocage de l'accès au service d'initiation de paiement et au service d'information sur les comptes

La Banque peut refuser aux prestataires de services d'information sur les comptes ou aux prestataires de services d'initiation de paiement l'accès à un compte de paiement du client si des raisons objectives et dûment justifiées en rapport avec l'accès non autorisé ou frauduleux du prestataire de services d'information sur les comptes ou du prestataire de services d'initiation de paiement au compte de paiement, y compris l'initiation non autorisée ou frauduleuse d'une opération de paiement, justifient ce refus. La Banque informe le client de ce refus d'accès par les moyens convenus. Les informations sont si possible fournies avant, mais au plus tard immédiatement après, le refus d'accès. La Banque ne peut pas donner de raisons si cela constituerait un non-respect d'obligations légales. Dès que les motifs de refus d'accès n'existent plus, la Banque lève le blocage de l'accès. Elle en informe le client sans délai.

10. Responsabilité

10.1 Responsabilité de la Banque en cas d'exécution d'un ordre non autorisé et pour un ordre non exécuté, mal exécuté ou retardé

La responsabilité de la Banque pour un ordre non autorisé et pour un ordre non exécuté, mal exécuté ou retardé est régie par les conditions spéciales convenues pour le type d'ordre concerné (conditions de transfert, par exemple, ou conditions relatives aux titres).

10.2 Responsabilité du client en cas d'utilisation abusive de ses éléments d'authentification

10.2.1 Responsabilité du client pour les opérations de paiement non autorisées avant l'avis de blocage

(1) Si des opérations de paiement non autorisées effectuées avant la notification de blocage résultent de l'utilisation d'un élément d'authentification égaré, volé ou perdu de toute autre manière, ou de toute autre utilisation abusive d'un élément d'authentification, le client est responsable des pertes subies par la Banque de ce fait à concurrence d'un montant de 50,00 EUR, que le Participant soit coupable ou non.

(2) Le client n'est pas responsable des pertes visées au paragraphe 1 si

- il lui est impossible de remarquer l'égarement, le vol ou toute autre perte ou tout autre usage abusif de l'élément d'authentification, ou
- l'égarement de l'élément d'authentification a été causée par un employé, un agent, une succursale d'un prestataire de services de paiement ou toute autre partie à laquelle les services ont été sous-traités.

(3) Si des opérations de paiement non autorisées sont effectuées avant l'avis de blocage et que le participant a agi frauduleusement ou intentionnellement en violation de ses obligations de notification et de diligence ou qu'il l'a fait à la suite d'une négligence grave, le client doit supporter intégralement les pertes qui en résultent. Le Participant peut se rendre coupable de négligence grave, notamment s'il a manqué à l'un de ses devoirs de diligence conformément

- à l'Article 7.1 paragraphe 2,
- à l'Article 7.1 paragraphe 4,
- à l'Article 7.3 ou
- à l'Article 8.1 paragraphe 1

des présentes Conditions.

(4) Nonobstant les paragraphes 1 et 3, le client n'est pas responsable des pertes si la Banque n'a pas demandé une authentification forte du client conformément aux dispositions du Code monétaire et financier. Une authentification forte du client nécessite notamment l'utilisation de deux éléments indépendants l'un de l'autre des catégories connaissance, possession ou inhérence (cf. Article 2 paragraphe 3 des présentes Conditions).

(5) La responsabilité pour les pertes subies pendant la période à laquelle s'applique la limite de transaction est limitée à la limite de transaction convenue.

(6) Le client n'est pas responsable des pertes visées aux paragraphes 1 et 3 si le Participant n'a pas pu émettre son avis de blocage parce que la Banque n'a pas réussi à mettre en œuvre un moyen de recevoir l'avis de blocage.

(7) Les paragraphes 2 et 4 à 6 ne s'appliquent pas si le Participant a agi frauduleusement.

(8) Si le client n'est pas un consommateur, les dispositions suivantes s'appliquent en plus :

Le client est responsable des dommages dus à des opérations de paiement non autorisées au-delà de la limite de responsabilité de 50 EUR conformément aux paragraphes 1 et 3 si le Participant a négligemment ou intentionnellement violé ses obligations de notification et de diligence raisonnable au titre des présentes Conditions.

La limitation de responsabilité prévue au paragraphe 2, premier Article, ne s'applique pas.

10.2.2 Responsabilité du client pour les transactions non autorisées en dehors des services de paiement (ex. opérations sur titres) avant l'avis de blocage

Si des opérations non autorisées en dehors des services de paiement (par exemple des opérations sur titres) avant l'avis de blocage résultent de l'utilisation d'un élément d'authentification perdu ou volé ou de toute autre utilisation abusive de l'élément d'authentification et si la Banque subit une perte de ce fait, le client et la Banque sont responsables conformément aux principes légaux de la négligence contributive.

10.2.3 Responsabilité de la Banque après l'avis de blocage

Dès que la Banque reçoit un avis de blocage d'un Participant, elle assume la responsabilité de toutes les pertes subies à la suite d'opérations bancaires en ligne non autorisées. Cela ne s'applique pas si le Participant a agi avec une intention frauduleuse.

10.2.4 Exclusion de responsabilité

Les demandes en responsabilité sont exclues si les circonstances sur lesquelles se fonde la demande résultent d'un événement inhabituel et imprévisible sur lequel la partie qui invoque l'événement n'a aucune influence et dont les conséquences n'auraient pu être évitées par elle malgré toute la diligence déployée.

11. Explications de la Banque et relevés de compte

(1) Dans le cadre de la relation d'affaires entre la Banque et le client, l'Interface Utilisateur est le dispositif de réception convenu avec le client. Les notifications et explications de la Banque sont mises à la disposition du client par l'intermédiaire de l'Interface Utilisateur sous forme électronique, pour autant que la forme écrite n'ait pas été expressément convenue avec le client ou qu'elle constitue une exigence légale.

(2) Les notifications et explications concernant la relation d'affaires avec la Banque sont fournies au client par la Banque sous forme cryptée via l'Interface Utilisateur. Les notifications et les explications fournies via l'Interface Utilisateur ne sont envoyées par la poste que si cela constitue une obligation légale.

Indépendamment de l'utilisation de l'Interface Utilisateur comme moyen de communication électronique par le client, la Banque est autorisée à envoyer des notifications et des explications individuelles ou, en cas de problèmes techniques, toutes les notifications et explications par courrier ou sous une autre forme au client, si elle l'estime opportun compte tenu des intérêts de ce dernier.

La Banque informe le client de la disponibilité de certains documents via l'Interface Utilisateur elle-même ou via le partenaire de la Banque par e-mail, SMS ou tout autre moyen convenu avec le client.

(3) Le client est tenu d'ouvrir régulièrement et rapidement les notifications et explications via l'Interface Utilisateur et d'en vérifier le contenu dès que la Banque l'a informé de la disponibilité de ces notifications et explications. Toute inexactitude doit être notifiée à la Banque immédiatement, au plus tard six semaines après sa mise à disposition.

(4) Toutes les notifications et explications communiquées au client via l'Interface Utilisateur sont réputées avoir été reçues lorsque la Banque informe le client qu'elles sont disponibles et accessibles via l'Interface Utilisateur. La Banque et le client conviennent en conséquence que l'Interface Utilisateur est le dispositif utilisé par le client pour recevoir toutes les notifications et explications de la Banque, en particulier les relevés de compte et les comptes définitifs.

(5) La Banque veille à ce que les données figurant sur l'Interface Utilisateur ne puissent être modifiées. Cette obligation ne s'applique pas si les données sont stockées ou conservées en dehors de l'Interface Utilisateur. En raison des paramètres spécifiques du matériel et des logiciels, l'apparence d'une impression ne correspondra pas toujours à la présentation à l'écran.

(6) La Banque sauvegarde de manière permanente tous les documents qu'elle fournit via l'Interface Utilisateur pendant la durée de la relation d'affaires. Lorsque la relation d'affaires prend fin, le client peut exiger de la Banque des copies des relevés de compte et des comptes définitifs, moyennant le paiement d'une commission que la Banque peut fixer à sa discrétion.

(7) Les obligations d'information à l'égard des consommateurs résultant à la fois du Code monétaire et financier et du Code de la consommation sont inapplicables si le client n'est pas un consommateur.