Conditions applicables au service de banque en ligne

saarLB

Landesbank Saar
Ursulinenstraße 2, 66111 Saarbrücken

Version septembre 2022

1 Prestations

1) Grâce au service de banque en ligne (« Online-Banking »), le titulaire d'un compte ou d'un compte-titres et ses mandataires ont la possibilité d'effectuer des opérations bancaires dans les limites fixées par la banque. En outre, ce service leur permet de consulter en ligne des informations de la banque. Conformément au § 675f alinéa 3 du BGB (code civil allemand), ils peuvent également recourir à un service d'initiation de paiement selon le § 1 al. 33 de la loi allemande sur la surveillance des services de paiement (ZAG) et à un service d'information sur les comptes conformément au § 1 al. 34 de la loi précitée. Ils peuvent enfin recourir à d'autres services de tiers qu'ils sélectionnent.
(2) Les titulaires de compte/de comptes-titres et leurs mandataires sont désignés ensemble sous le vocable « participant » tandis que les comptes et comptes-titres sont désignés ci-après sous le vocable unique « compte », sauf stipulation expresse contraire.
(3) Les plafonds d'opérations convenus par acte séparé avec la banque s'appli- quent à l'utilisation du service de banque en ligne. Le titulaire du compte et sa banque peuvent convenir d'une modification de ces plafonds par acte séparé. Les mandataires ne peuvent conclure que la réduction de ces plafonds.

2 Conditions d'utilisation du service de banque en ligne

(1) Le participant peut utiliser le service de banque en ligne après son authentification par la banque.
(2) L'authentification est la procédure convenue avec la banque de façon séparée, qui permet à la banque de vérifier l'identité du participant ou le caractère autorisé de l'usage d'un moyen de paiement convenu. Au moyen des éléments d'authentification convenus à cet effet, le participant peut établir vis à vis de la banque son habilitation, accéder à des informations (cf. art. 3) et passer des ordres (cf. art. 4).
(3) Les éléments d'authentification sont :
- des éléments de connaissance, c'est à dire quelque chose que seul le participant connait (par ex. numéro d'identification personnel [PIN]),
- des éléments de possession, c'est-à-dire quelque chose que seul le participant détient (par ex. appareil permettant de générer ou de recevoir des numéros de transaction à usage unique [TAN], qui prouvent la possession du participant, comme la carte bancaire avec générateur de TAN ou le terminal mobile), ou
- des éléments d'être, c'est à dire quelque chose que le participant est (inhérence, par ex. empreinte digitale en tant que caractéristique biométrique du participant).
(4) L'authentification du participant est réalisée par la transmission par ce dernier à la banque de l'élément de connaissance, de la preuve de l'élément de possession et/ou de la preuve de l'élément d'être, conformément aux demandes de la banque.
.

3 Accès au service de banque en ligne

(1) Le participant peut accéder au service de banque en ligne si
– il indique son identifiant-participant individuel (p. ex. n° de compte, nom d'utilisateur)
– il s'identifie par l'utilisation de l'élément/des éléments d'authentification exigé(s) par la banque, et
– l'accès au service n'est pas bloqué (cf. art. 8.1 et 9).
Une fois l'autorisation d'accès au service de banque en ligne accordée, il est possible de consulter diverses informations et d'émettre des ordres conformément à l'article 4.
(2) Pour accéder à des données de paiement sensibles au sens du § 1 alinéa 26 première phrase de la ZAG (par ex. aux fins de modification de l'adresse du titulaire du compte), la banque demande au participant de s'identifier en utilisant un moyen d'authentification supplémentaire si lors de l'accès au service un seul moyen d'authentification avait été demandé. Le nom du titulaire du compte et le numéro de compte ne constituent pas des données de paiement sensibles pour les services d'initiation de paiement et d'informations sur le compte utilisés par le participant (§ 1 alinéa 26, deuxième phrase, ZAG).

4 Ordres

4.1 Passation d'ordres
Le participant doit marquer son consentement à un ordre (par ex. un virement) pour qu'il puisse produire effet (autorisation). Il doit pour cela utiliser les moyens d'authentification qui lui sont demandés (p. ex. indication d'un TAN comme preuve de l'élément de possession).
La banque confirme la réception de l'ordre par le service en ligne.
4.2 Révocation d'ordres
Le caractère révocable ou non d'un ordre est déterminé par les conditions applicables en fonction du type d'ordre (p. ex. conditions applicables aux virements). La révocation d'ordres ne s'effectue pas par le biais du service de banque en ligne, sauf si une telle possibilité est expressément prévue par la banque.

5 Traitement des ordres par la banque

(1) La banque traite les ordres aux jours ouvrés mentionnés, pour chaque type d'ordre (p.ex. virement), sur la page Online-Banking ou dans le « Recueil des tarifs et des prestations », dans le cadre d'une exécution normale.
Si l'ordre est reçu au-delà de la date mentionnée sur la page Online-Banking ou dans le « Recueil des tarifs et des prestations » (délai d'acceptation), ou si la date de réception de l'ordre ne correspond pas à un jour ouvré, tel que défini par la page Online-Banking de la banque ou le « Recueil des tarifs et des prestations », l'ordre est réputé reçu le jour ouvré suivant. Ce n'est qu'à ce jour ouvré que commencera le traitement de l'ordre.
(2) La banque exécute l'ordre si les conditions d'exécution suivantes sont réunies :
– Le participant a autorisé l'ordre (cf. art. 4.1)
– Le participant est habilité à passer le type d'ordre concerné (p.ex. opérations sur titres)
– Le format des données propre au service de banque en ligne est respecté
– Le plafond des opérations du service de banque en ligne convenu par acte séparé n'est pas dépassé (cf. art. 1 § 3)
– Les conditions d'exécution posées par les conditions applicables au type d'ordre concerné sont réunies (p. ex. une provision suffisante conformément aux con- ditions applicables aux virements).
Si les conditions d'exécution selon la première phrase sont réunies, la banque exé- cute l'ordre conformément aux conditions applicables au type d'ordre concerné (p.ex. Conditions applicables aux virements, Conditions applicables aux opérations sur titres).
(3) Si les conditions d'exécution selon le paragraphe 2, phrase 1 ne sont pas réu- nies, la banque n'exécute pas l'ordre. Par le biais du service de banque en ligne, elle met à disposition du participant une information concernant la non-exécution et, si possible, ses motifs et la procédure à suivre pour corriger les erreurs l'ayant entraînée.

6 Information du titulaire du compte sur les opérations effectuées en ligne

La banque informe le titulaire du compte au moins une fois par mois des opérations effectuées via le service de banque en ligne selon le mode de communication convenu pour les informations relatives au compte.

7 Obligations du participant

7.1 Protection des éléments d'authentification
(1) Le participant doit prendre toutes les mesures raisonnablement réalisables pour protéger ses éléments d'authentification (cf. art. 2) contre tout accès non autorisé. A défaut, existe le risque que le service de banque en ligne soit utilisé de manière abusive ou de toute autre façon non autorisée (cf. art. 3 et 4).
(2) Pour la protection de ses éléments d'authentification, le participant doit avant tout prendre les mesures suivantes :
(a) les éléments de connaissance comme le PIN doivent être tenus secrets ; en particulier, ils ne doivent pas être
- communiqués verbalement (par ex. par téléphone ou personnellement),
- retransmis en dehors du service de banque en ligne au format texte

(par ex. par email, service de messagerie),
- stockés électroniquement sous forme non sécurisée (par ex. stockage du PIN en texte clair dans l'ordinateur ou dans le terminal mobile),
- notés sur un appareil ou conservé en copie ensemble avec un appareil servant d'élément de possession (p. ex. carte bancaire avec générateur TAN, terminal mobile, carte de signature électronique) ou à la vérification d'un élément d'être (p. ex. terminal mobile avec application pour Online-Banking et capteur d'empreinte digitale).

(b) Les éléments de possession comme par ex. la carte bancaire avec générateur TAN doivent être protégés contre tout usage abusif, en particulier
- les cartes bancaires avec générateur TAN ou les cartes de signature électronique doivent être conservées à l'abris de tout accès non autorisé d'autres personnes,
- il convient de s'assurer que des personnes non autorisées ne puissent accéder au terminal mobile du participant (p. ex. téléphone portable),
- il faut veiller à ce que d'autres personnes ayant accès au terminal mobile (par ex. téléphone portable) ne puissent pas utiliser l'application sensible servant au service de banque en ligne (p. ex. les applications Online-Banking ou d'authentification),
- l'application sensible servant au service de banque en ligne (par ex. les applications Online-Banking ou d'authentification) se trouvant sur le terminal mobile du participant doit être désactivée avant que le participant ne transfère la possession de ce terminal (p. ex. par voie de vente ou de mise au rebut du téléphone portable),
- les preuves de l'élément de possession (par ex. TAN) ne doivent pas être retransmises en dehors du service de banque en ligne verbalement (p. ex. par téléphone) ou au format texte (p. ex. par email, service de messagerie), et
- le participant, qui a reçu de la banque un code d'activation de l'élément de possession (p. ex. téléphone portable avec application Online-Banking) doit conserver ce dernier à l'abris de l'accès non autorisé d'autres personnes ; à défaut existe le risque que d'autres personnes puissent activer l'appareil en tant qu'élément de possession pour le service de banque en ligne.

(c) Des éléments d'être, comme par exemple l'empreinte digitale du participant, ne peuvent être utilisés comme élément d'authentification pour le service Online-Banking sur un terminal mobile du participant que si aucun élément d'être d'autres personnes n'est stocké sur ce terminal. Si un élément d'être d'une autre personne est stocké sur le terminal mobile servant au service Online-Banking, c'est l'élément de connaissance (p. ex. PIN) fourni par la banque pour le service Online-Banking qui doit être utilisé et non l'élément d'être stocké sur le terminal mobile.

(3) Sans préjudice des obligations de prudence évoquées aux paragraphes 1 à 2, le participant peut utiliser ses éléments d'authentification à l'égard d'un service d'initiation de paiement ou d'information sur le compte qu'il a choisi ainsi que d'un autre service de tiers (cf. art. 1 § 1 phrases 3 et 4). Le participant doit choisir les autres services de tiers avec le plus grand soin.

7.2. Consignes de sécurité de la banque

Le participant doit respecter les consignes de sécurité figurant sur la page Online-Banking de la banque, en particulier les mesures de protection de l'équipement informatique et des logiciels utilisés.

7.3 Vérification des données de l'ordre récapitulées par la banque

La banque notifie au participant les données d'ordre qu'elle a reçues (p. ex. montant, n° de compte du bénéficiaire, code d'identification des titres) par le biais de l'appareil du participant désigné par convention séparée (p. ex. téléphone mobile, lecteur de carte à puce avec écran). Le participant doit vérifier que les données affichées sont conformes aux données prévues pour l'ordre avant de les confirmer.

8 Obligations de déclarer et d'informer

8.1 Opposition

(1) Si le participant constate
- la perte ou le vol d'un élément de possession permettant l'authentification (par ex. carte bancaire avec générateur de TAN, terminal mobile, carte de signature électronique) ou
- l'utilisation frauduleuse ou toute autre utilisation non autorisée de son élément d'authentification,

il doit en informer immédiatement la banque (opposition). Le participant peut également former une opposition à tout moment en utilisant les moyens de communication communiqués séparément.

(2) Le participant doit déclarer à la police sans délai tout vol ou usage frauduleux 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 faire opposition.

8.2 Information relative à des ordres non autorisés ou mal exécutés

Si le titulaire du compte constate l'exécution d'un ordre non autorisé ou une exé- cution erronée, il doit en informer la banque immédiatement.

9 Blocage de l'utilisation du service

9.1 Blocage à l'initiative du participant

À la demande du participant, notamment dans le cas d'une opposition confor- mément à l'article 8.1, la banque bloque
– l'accès au service de banque en ligne, soit pour ce seul participant, soit pour tous les participants, ou
– ses éléments d'authentification servant au service Online-Banking.

9.2 Blocage à l'initiative de la banque

(1) La banque peut bloquer l'accès au service de banque en ligne d'un participant si
– elle est en droit de résilier le contrat relatif au service de banque en ligne pour un motif grave,
– cela est justifié par des raisons objectives en rapport avec la sécurité des éléments d'authentification du participant ou
– il existe un soupçon d'utilisation non autorisée ou frauduleuse d'un élément d'authentification.

(2) La banque en informera le titulaire du compte selon le moyen convenu en indiquant les motifs de sa décision, si possible avant de procéder au blocage, ou au plus tard immédiatement après. La banque peut ne pas indiquer de motif si les dispositions légales le lui interdisent.

9.3 Déblocage

La banque désactivera le blocage ou délivrera de nouveaux éléments d'authentification dès lors que les raisons justifiant le blocage n'existent plus. Elle en informera le titulaire du compte sans délai.

9.4 Blocage automatique d'un élément de possession

(1) Une carte à puce équipée de la fonction signature électronique se bloque auto- matiquement au bout de trois saisies consécutives d'un code de signature élec- tronique erroné.

(2) Un générateur de TAN intégré dans une carte à puce (p. ex. carte bancaire) qui nécessite la saisie d'un code d'utilisation personnel se bloque automatiquement au bout de trois saisies consécutives d'un code erroné.

(3) Les éléments de possession mentionnés aux paragraphes 1 et 2 ne peuvent alors plus être utilisés pour le service de banque en ligne. Le participant peut contacter la banque afin de rétablir les possibilités d'utilisation du service.

9.5 Blocage d'accès pour les services d'initiation de paiement et d'information sur le compte

La banque peut refuser l'accès à un compte de paiement du titulaire à un prestataire de services d'information sur le compte ou de services d'initiation de paiement si des raisons objectives et dûment justifiées, liées à un accès au compte non autorisé ou frauduleux par le prestataire, y compris l'initiation non autorisée ou frauduleuse d'un paiement, le justifient. La banque informera le titulaire d'un tel refus d'accès par le moyen convenu. L'information est donnée si possible avant le refus d'accès, ou au plus tard immédiatement après. La banque peut ne pas indiquer de motif si les dispositions légales le lui interdisent. La banque désactive le blocage dès que les raisons justifiant le refus d'accès n'existent plus. Elle en informe le titulaire du compte sans délai.

10 Responsabilité

10.1 Responsabilité de la banque en cas d'exécution d'un ordre non autorisé, de non-exécution, de mauvaise exécution ou d'exécution tardive d'un ordre

En cas d'ordre non autorisé, de non-exécution, de mauvaise exécution ou d'exécution tardive d'un ordre, la responsabilité de la banque est régie par les conditions convenues pour le type d'ordre concerné (p. ex. Conditions applicables aux virements, Conditions applicables aux opérations sur titres).

10.2 Responsabilité du titulaire du compte en cas d'utilisation frauduleuse d'un élément d'authentification

10.2.1 Responsabilité du titulaire du compte en cas d'opérations de paiement non autorisées effectuées avant la demande d'opposition

(1) Si les opérations de paiement non autorisées et effectuées avant l'opposition sont dues à la perte, au vol ou à tout autre disparition de l'élément d'authentification ou à son utilisation frauduleuse ou non autorisée, le titulaire du compte supporte le préjudice occasionné à la banque jusqu'à un montant de 50 euros, sans qu'il y ait lieu de distinguer si le participant a commis une faute ou non.

(2) Le titulaire du compte ne supporte pas la responsabilité prévue au paragraphe 1 si

– il n’a pas été possible au participant de détecter la perte, le vol, la dépossession ou toute autre utilisation irrégulière de l’élément d’authentification avant l’opération de paiement non autorisée, ou
– la perte de l’élément d’authentification a été causée par un employé, un agent ou une succursale ou agence d’un prestataire de services de paiement ou tout autre établissement auquel les activités du prestataire de services de paiement ont été externalisées.
(3) Si des opérations de paiement non autorisées sont effectuées avant l’opposition et si le participant n’a pas respecté, intentionnellement ou par négligence grave, les consignes de sécurité et d’information énoncées aux présentes Conditions ou s’il a agi avec une intention frauduleuse, le titulaire du compte supporte le préjudice occasionné dans sa totalité, par dérogation aux § 1 et 2. Une négligence grave peut résulter notamment du fait que le participant a manqué à l’une de ses obligations de vigilance énoncées aux
- article 7.1 § 2,
- article 7.3. ou
- article 8.1 § 1.
(4) Par dérogation aux paragraphes 1 et 3, si la banque n’a pas exigé du participant une authentification forte selon le § 1 al. 24 ZAG, le titulaire du compte n’est pas tenu à réparation du dommage. Une authentification forte du client exige notamment l’utilisation de deux éléments d’authentification indépendants l’un de l’autre appartenant aux catégories Savoir, Possession ou Être (cf. art. 2 § 3).
(5) La responsabilité pour les dommages occasionnés au cours de la période à laquelle s’applique le plafond des opérations se limite au plafond respectivement convenu.
(6) Le titulaire du compte n'est pas tenu à réparation des dommages visés par les paragraphes 1 et 3, si le dommage est dû à l'impossibilité pour le participant de faire opposition selon l’article 8.1 du fait de la banque qui n'a pas mis en œuvre les moyens de recevoir une telle opposition.
(7) Les paragraphes 2 et 4 à 6 ne s’appliquent pas si le participant a agi dans une intention frauduleuse.
(8) Si le titulaire du compte n’est pas un consommateur, s’applique en outre ce qui suit :
– le titulaire du compte répond des dommages causés par des paiements non auto- risés même au-delà de la limite de 50 euros visée aux paragraphes 1 et 3 si le participant a manqué par négligence ou intentionnellement à ses devoirs d’opposition et de prudence résultant des présentes Conditions.
– la limitation de responsabilité du paragraphe 2 premier tiret ne s’applique pas
10.2.2 Responsabilité du titulaire du compte en cas d’opérations non autorisées en dehors des services de paiement (p. ex. transactions sur titres), effectuées avant l’opposition
Si des opérations non autorisées autres que des services de paiement (p. ex. transactions sur titres) effectuées avant l’opposition sont dues à la perte ou au vol, ou à une utilisation frauduleuse, d’un élément d’authentification, et s’il en résulte un dommage pour la banque, le titulaire du compte et la banque en assument la responsabilité conformément aux dispositions du droit allemand de la co-responsabilité.

10.2.3 Responsabilité à partir de l’opposition
Dès lors que la banque a reçu une opposition d’un participant, elle assume tous les dommages survenus qui résultent de l’exécution non autorisée après l’opposition d’opérations par le service de banque en ligne. Ceci ne s’applique pas si le partici- pant a agi avec une intention frauduleuse.
10.2.4 Exclusion de responsabilité
Toute indemnisation est exclue si le dommage résulte d’un événement extra- ordinaire et imprévisible échappant au contrôle de la partie invoquant la prise en compte de cet événement, dont les suites auraient été inévitables malgré tous les efforts déployés.

11 Résolution extrajudiciaire des litiges et autres possibilités de réclamation

Pour le règlement des litiges avec la banque, le titulaire du compte peut s'adresser aux instances de résolution des litiges et de réclamation mentionnées dans le « Recueil des tarifs et des prestations ».