# POLITIQUE DE LA PROTECTION DE LA VIE PRIVÉE

DE SANTANDER CONSUMER FINANCE, S.A - SUCCURSALE EN BELGIQUE

# Table des matières

1. Responsable du traitement ..... 2
2. Délégué à la protection des données (‘Data Protection Officer’) ..... 2
3. Informations recueillies et traitées par la Banque ..... 3
4. Collecte de données de navigation ..... 3
5. Collecte de vos données à caractère personnel et finalités des traitements ..... 4
6. Respect des principes de protection des données ..... 7
7. Le Groupe Santander ..... 7
8. Partenaires ..... 8
9. Sécurité / confidentialité ..... 9
10. Période de rétention de vos données ..... 11
11. Protection et confidentialité ..... 11
12. Exercice de vos droits ..... 12
13. Comment exercer vos droits ? ..... 13

## 1. Responsable du traitement

Santander Consumer Finance, succursale en Belgique, dont le siège social est situé en Belgique, à 9820 Merelbeke, 81 Guldensporenpark et Santander Consumer Finance SA, dont le siège social est sis en Espagne, à 28660 Boadilla del Monte, Avenida de Cantabria s/n sont conjointement responsables de vos données à caractère personnel.

Santander Consumer Finance SA n'aura pas accès à vos données personnelles sauf dans les cas particuliers décrits dans la section Groupe Santander. Cependant, les décisions relatives aux finalités des traitements sont prises conjointement par les deux entités (Santander Consumer Finance, succursale en Belgique et Santander Consumer Finance, S.A.).

Cette politique vous informe du traitement que Santander Consumer Finance, succursale en Belgique et Santander Consumer Finance SA (ci-après ensemble « la Banque ») réservent à vos données personnelles lorsque vous naviguez sur son site internet, effectuez une ouverture de compte, devenez client ou clôturez un compte, et de vos droits quant aux informations recueillies et utilisées.

La Banque apprécie la confiance que vous lui accordez et s'engage à tout mettre en œuvre pour maintenir la confidentialité des informations que vous lui transmettez.

La Banque s'engage également à préserver la légalité, la proportionnalité et la transparence de la gestion de vos données personnelles et travaille en permanence à l'amélioration de ses services.

Vous pouvez, en tant que titulaire de ces données personnelles, exercer vos droits d'opposition, d'accès, de rectification et de portabilité contre de chacun des responsables du traitement, selon les modalités prévues par cette politique (voir section Comment exercer vos droits ?). Vous pouvez envoyer toutes vos questions concernant la protection de vos données à caractère personnel à l'adresse électronique suivante : dataprotection@santanderconsumerbank.be.

L'Autorité espagnole de protection des données agira en tant que principale autorité de contrôle. En cas de consultation ou de plainte, vous pourrez adresser directement vos requêtes sans distinction à l'autorité belge de protection des données :
(https://www.autoriteprotectiondonnees.be/citoyen/agir/introduire-une-plainte)
ou à l'autorité espagnole de protection des données :
(https://sedeagpd.gob.es/sede-electronica-web/vistas/infoSede/tramitesCiudadano.jsf).

## 2. Délégué à la protection des données ('Data Protection Officer')

La Banque a désigné un délégué à la protection des données qui peut être contacté de la manière suivante : dataprotection@santanderconsumerbank.be ou par courrier postal à l'adresse suivante : Santander Consumer Finance SA, Avenida de Cantabria s/n, 28660 Boadilla del Monte (Espagne).

Ce délégué à la protection des données est compétent :

- Pour informer et conseiller la Banque, ses administrateurs ainsi que les membres des comités d'avis constitués dans le cadre de la gestion et de l'exécution de ses activités, sur leurs en vertu de la législation et de la réglementation en matière de protection des données ;

- Pour contrôler le respect de la législation et de la réglementation en matière de protection des données et de la politique de traitement et de protection des données dans le cadre de la gestion et de l'exécution des activités de la Banque, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant ;

- Pour donner des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et pour en contôler l'exécution ;

- Pour coopérer avec l'Autorité de Protection des Données ;
- Pour servir de point de contact pour :
    - les clients qui veulent contacter le Délégué à la protection des données pour toutes les questions liées au traitement de leurs données à caractère personnel et à l'exercice de leurs droits ;
    - les clients ou toute autre personne qui constate un incident ou une violation en lien avec le traitement des données à caractère personnel dans le cadre de la gestion et de l'exécution des activités de la Banque et qui doivent, entre autres, en informer le Délégué à la protection des données ;
    - l'Autorité de Protection des Données en ce qui concerne les questions liées au traitement ;
- pour tenir compte du risque associé aux opérations de traitement, compte tenu de la nature, de la portée, du contexte et des finalités du traitement.

Le Délégué à la protection des données est soumis au secret professionnel et à une obligation de confidentialité en ce qui concerne l'exercice de ses missions.

## 3. Informations collectées et traitées par la Banque

La Banque collecte et utilise différents types de données que vous transmettez volontairement ou qui sont générées pendant de la relation contractuelle. La Banque utilise aussi des données qui sont récoltées sur la base de votre consentement préalable (par exemple, en acceptant les cookies commerciaux lorsque vous naviguez sur le site internet de la Banque).

## 4. Collecte de données de navigation

Ces données sont obtenues de manière automatique.

En principe, les données de navigation peuvent être individuelles (se rapportant à vous seul(e)) ou agrégées (concernant un groupe d'utilisateurs) et s'obtiennent automatiquement via l'usage de « cookies » et par traitement des adresses IP.

Les cookies sont des blocs de données conservés dans votre ordinateur, que la Banque utilise pour de faciliter vos futures visites en fonction des consultations observées lors de vos visites antérieures. Les cookies utilisés par la Banque sont codés et contiennent une signature numérique unique pour empêcher toute modification.

La Banque utilise ces données sous une forme agrégée afin d'enquêter sur l'historique et les schémas de consultation de son site internet. Nous utilisons le service Google (plus concrètement Google Analytics) à des fins statistiques (données anonymisées, c'est-à-dire analysées globalement pour en faire un résumé anonymisé).).

Google Analytics utilise des « cookies », qui sont des fichiers de texte situés sur votre ordinateur, pour aider le site internet à analyser votre utilisation. Les informations générées par les cookies concernant votre utilisation du site internet (y compris votre adresse IP) seront directement transmises et archivées par Google sur des serveurs situés aux États-Unis.

Dans les paramètres du système, la Banque a introduit une période de rétention pour les informations stockées par Google et a sélectionné le cryptage de ses données, de sorte que Google Analytics ne peut voir vos données que sous une forme cryptée.

Google utilisera cette information sur son propre compte afin de garder une trace de votre utilisation du

site internet, de compiler des rapports sur l'activité du site internet et de fournir d'autres services liés à l'activité du site internet et à l'utilisation d'Internet. Google peut transmettre ces informations à des tiers lorsque cela est requis par la loi ou lorsque ces tiers traitent ces informations pour le compte de Google. Google n'associera pas votre adresse IP à d'autres données qu'il détient.

Vous pouvez refuser le traitement de données ou d'informations en refusant l'utilisation de cookies dans la configuration de votre navigateur. Google Analytics a une extension pour le navigateur qui permet aux utilisateurs d'accepter ou de désactiver le traçage, le « Module complémentaire de navigateur pour la désactivation de Google Analytics ». Google a sa propre politique de protection des données à caractère personnel. Vous pouvez lire plus de détails à ce sujet sur la politique de vie privée de Google. Nous vous recommandons de prendre le temps de la lire ces informations attentivement.

En outre, nous devons vous informer que nous avons activé Google Signals dans notre compte Google Analytics. Google Signals est un programme intégré à Google Analytics qui utilise les données de session des sites et des applications que Google associe aux utilisateurs qui se sont connectés à leur compte Google et qui ont activé la personnalisation des annonces.

Cela signifie que Google Analytics peut associer les données de session qu'il recueille aux informations des utilisateurs connectés à Google afin de fournir des informations agrégées et anonymes sur les comportements des utilisateurs à travers les appareils et sur leurs données démographiques. Les informations Google qui peuvent être collectées comprennent l'historique des recherches, la localisation de l'utilisateur final et des données provenant de sites partenaires de Google, ce qui permet d'obtenir des informations plus spécifiques et plus complètes sur l'utilisateur que Google Analytics.

En conséquence, nous recevons des rapports améliorés et des informations plus utiles sur le comportement, les intérêts et les caractéristiques démographiques d'un utilisateur, quel que soit l'appareil utilisé. Celles-ci comprennent votre âge, la langue que vous parlez, votre lieu de résidence ou votre sexe.

Ces rapports nous aident également à mieux évaluer le comportement de nos utilisateurs, ainsi que leurs souhaits et intérêts. Nous pouvons ainsi optimiser et personnaliser nos produits et services pour eux. Par défaut, ces données expirent au bout de 26 mois. Veuillez noter que ces données ne sont collectées que si l'utilisateur a accepté la publicité personnalisée dans son compte Google. Les informations conservées sont toujours exclusivement des données résumées et anonymes, et jamais des données sur des personnes individuelles. Vous pouvez gérer ou supprimer ces données dans votre compte Google.

Consultez plus d'informations sur Google Signals.

Google a sa propre politique de confidentialité. Vous pouvez en savoir plus à l'adresse suivante : www.google.com/policies/privacy. Nous vous recommandons de prendre le temps de la lire attentivement.

Pour plus d'informations, la Banque vous invite à consulter sa politique en matière de cookies.

## 5. Collecte de vos données à caractère personnel et finalités des traitements

La définition des données à caractère personnel se réfère à toute information numérique, alphabétique, graphique, photographique, acoustique ou toute autre information concernant des individus identifiés ou identifiables (telles que des données biométriques). Les données anonymes ne seront jamais considérées comme des données personnelles.

Les données à caractère personnel sont recueillies et traitées de différentes manières :

(a) Afin d'exécuter la relation contractuelle en tenant compte du fait que vos données sont nécessaires pour ouvrir et gérer un compte d'épargne. Les données nécessaires sont celles indiquées dans le contrat : nom et prénom, adresse, adresse e-mail, numéro de

téléphone, date de naissance, sexe, langue, numéro de la carte d'identité (et date de validité), numéro de registre national, numéro du compte de référence, question de sécurité et réponse de sécurité. De même, les données issues de la relation contractuelle seront considérées comme nécessaires, à savoir : mouvements de compte, extraits de compte, calcul des intérêts, détails des virements, etc.

(b) Pour les personnes qui ont commencé une ouverture de compte sans avoir finalisé l'étape 2 (données de mon compte) et qui ont accepté de recevoir de l'aide pour continuer le processus d'ouverture de compte, nous utiliserons leur e-mail afin de leur offrir un accompagnement pour à finaliser le processus d'ouverture de compte.

(c) Dans le cadre d'une demande d'ouverture de compte, la loi oblige la Banque à vous demander de compléter un certain nombre de données personnelles permettant votre identification complète. Par la suite, vous devrez fournir à la Banque les documents prouvant l'authenticité de ces données personnelles (par exemple, en utilisant un lecteur d'authentification de carte d'identité électronique belge).

Les institutions financières doivent utiliser tous les moyens possibles pour prévenir et détecter le blanchiment de capitaux ou le financement du terrorisme et le signaler aux autorités conformément à la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme. La Banque doit vous identifier en tant que client, représentant/mandataire ou bénéficiaire ultime ; vérifier votre identité ; déterminer votre profil (en relation avec le risque de blanchiment de capitaux), ce qui implique de rassembler divers détails personnels et commerciaux, notamment vérifier si vous êtes une personne politiquement exposée.
Ce faisant, la Banque utilise les données personnelles que vous lui avez communiquées, ainsi que les données personnelles provenant d'autres sources (comme Dow Jones, Identifin ou même Internet) qui complètent votre identification (si applicable).

Les données à caractère personnel que vous nous transmettez volontairement lorsque vous arrivez à la fin du processus d'ouverture de compte sont les suivantes : nom et prénom, adresse, adresse e-mail, numéro de téléphone portable, lieu de naissance, date de naissance, pays de naissance, nationalité, sexe, état civil, profession, secteur d'activité, mandat politique ou une fonction publique importante (PEP), numéro de la carte d'identité (et date de validité), numéro de registre national, numéro du compte de référence, résidence fiscale, exonération fiscale en matière de précompte mobilier.

Dans le cadre de l'utilisation de votre compte d'épargne, la Banque vérifie vos actions et transactions et contrôle certaines transactions pour prévenir et détecter le blanchiment de capitaux. Les banques doivent également comparer les données personnelles des clients par rapport aux listes de sanctions. Dans certains cas, des documents additionnels peuvent être demandés (par exemple, fiche de paie) et des paiements peuvent être retenus.
Les banques doivent également avoir une vision globale du risque par client au plus haut niveau, c'est la raison pour laquelle la Banque doit transmettre vos données au niveau intragroupe pour pouvoir vérifier si vous avez d'autres comptes au sein du Groupe Santander et pouvoir vous attribuer le niveau de risque adéquat (plus d'informations dans la section Groupe Santander).

De la même manière, vos données seront traitées conformément à la loi du 16 décembre 2015 réglant la communication des renseignements relatifs aux comptes financiers, par les institutions financières belges et le SPF Finances (Réglementation FATCA et CRS). Les données à caractère personnel utilisées à ces fins sont : nom, adresse, numéro d'identification fiscale, date et lieu de naissance, le numéro de compte, le solde ou la valeur à la fin de l'année civile concernée et le montant total brut des intérêts déposés ou crédités.

(d) Au cours de la relation contractuelle, pour bien gérer vos comptes d'épargne et notre relation client, la Banque traite vos données sur base d'un intérêt légitime pour avoir une gestion interne plus efficace et pour avoir une vision consolidée de la relation client. Dans ce but, un dossier est créé concernant chaque client en reprenant toutes les actions engagées par le client pendant la relation contractuelle. La Banque dispose également des systèmes de gestion de relation avec les clients et peut traiter vos données dans des courriels et des rapports internes.
Les données personnelles qui sont collectées et consultées sont les mêmes que celles que vous nous avez fournies au moment de l'ouverture d'un compte, ainsi que les données récoltées pour des raisons de prévention de blanchiment de capitaux (comme expliqué dans les sections a) et b)). Nous disposons également de toutes les actions engagées par vous pendant la relation contractuelle (appels au call center, messages envoyés, vos mouvements de compte, vos calculs d'intérêts ainsi que toutes les informations que vous avez voulu partager avec nous).
La Banque se réserve le droit, sur base d'un intérêt légitime, d'enregistrer les conversations téléphoniques de son service à la clientèle, étant entendu que ces enregistrements sont conservés à des fins de contrôle de la qualité de son service à la clientèle et comme élément de preuve en cas de contestation. Par ailleurs, un message avertissant le client de la possibilité d'enregistrement de la conversation téléphonique précède celle-ci.
Vos données sont traitées seulement par les personnes autorisées dans la mesure où cela est nécessaire. Vous pouvez trouver plus d'informations à ce sujet dans la section Sécurité d'accès. Nous créons des rapports anonymisés afin d'utiliser la technique la moins intrusive pour analyser le comportement de notre clientèle sur base agrégée anonymisée (c'est-à-dire que vos données sont analysées globalement pour en faire un résumé anonymisé). Les données anonymisées sont celles qui apparaissent dans votre dossier client récoltées pendant les différents traitements décrits dans cette section.
Il peut vous être proposé de participer à des enquêtes qui ont généralement pour but de fournir des informations générales au sujet des produits ou services de la Banque. Dans la mesure où les informations obtenues via ces enquêtes se rapportent à vous-même, la participation à ces enquêtes est facultative. Cependant, vos données sont reprises dans des rapports anonymisés et traitées sur une base agrégée anonymisée (c'est-à-dire qu'elles sont analysées globalement pour en faire un résumé anonymisé).
Pour les personnes qui n'ont pas encore activé leur compte, nous utiliserons vos données pour vous offrir un accompagnement afin de finaliser le processus d'ouverture de compte.
Pour l'évaluation du fonctionnement de l'activité ainsi que du contrôle sur celui-ci, la Banque peut également effectuer des contrôles de qualité concernant le service donné.
La Banque procède également à l'enregistrement de copies de sécurité des données disponibles afin de pouvoir, en cas de perte pour n'importe quelle raison, récupérer les informations et continuer à vous fournir le service en garantissant l'intégrité de vos données.

(e) Nous mettons à votre disposition un service de plaintes. Afin de pouvoir donner suite à votre plainte, la loi nous oblige à accéder aux et traiter les informations nécessaires à cette fin. Les données traitées sont celles qui apparaissent dans votre dossier client récoltées pendant les différents traitements décrits ci-dessus.

(f) La Banque vous envoie également des informations commerciales par e-mail sur base du consentement explicite que vous nous accordez, si applicable. Pour cette fin nous utilisons votre adresse électronique.

(g) La Banque transmet également vos données au sein du Groupe Santander et à diverses entités publiques comme décrit dans la section Groupe Santander. Ces transmissions de données sont faites sur la base d'une obligation légale.

## 6. Respect des principes de protection des données

Vous pouvez être assuré(e) de la détermination de la Banque à respecter les principes imposés par la législation belge et européenne :

- Le principe de légalité : les données personnelles sont obtenues selon les exigences imposées par la réglementation applicable.
- Le principe de proportionnalité : les données personnelles ne seront traitées qu'à des fins (objectifs) nécessaires, appropriées et pertinentes.
- Le principe de transparence : les informations à fournir concernant la protection de vos données personnelles doivent être claires, concises, transparentes, compréhensibles et facilement accessibles, dans un langage clair et simple et sans ambiguïté, en d'autres termes, faciles à comprendre pour vous.
- Le maintien des finalités de la collecte : le traitement des données personnelles est limité aux finalités spécifiques, explicites et légitimes de la collecte de ces données.
- Le principe de minimisation et d'exactitude des données : le traitement des données personnelles sera adéquat, pertinent et limité à ce qui est nécessaire par rapport aux finalités spécifiques pour lesquelles les données personnelles sont traitées. De même, toutes les mesures raisonnables doivent être adoptées pour supprimer ou rectifier toutes les données personnelles qui peuvent être inexactes ou incomplètes, en ce qui concerne les finalités pour lesquelles elles sont traitées.
- Le délai de conservation des données : les données personnelles sont conservées d'une manière qui permet votre identification, dans le respect de la finalité de leur traitement et pour le temps strictement nécessaire à celui-ci.
- les principes d'intégrité, de confidentialité, de disponibilité et de résilience : garantir à toutes les personnes, dont les données personnelles sont collectées par la Banque, que ces dernières sont traitées avec le niveau de sécurité approprié, y compris la protection contre les activités de traitement non autorisées ou illégales et contre leur perte, destruction ou dommage accidentel, à travers des mesures organisationnelles, telles que la pseudonymisation[1] ou le chiffrement[2] des données personnelles.

## 7. Le Groupe Santander

Vos données personnelles sont transférées à d'autres entités du Groupe Santander et notamment à Santander Consumer Finance SA dont le siège social est sis en Espagne à Avenue de Cantabria s/n - Ciudad Grupo Santander, Boadilla del Monte (Madrid), dans le cadre de l'activité normale de la Banque,

---

[1] *La pseudonymisation consiste à transformer des données personnelles afin qu'elles ne puissent plus être attribuées à une personne spécifique sans l'utilisation d'informations supplémentaires, à condition que ces informations supplémentaires soient conservées séparément et fassent l'objet de mesures techniques et organisationnelles visant à garantir que les données ne sont pas attribuées à des personnes physiques. Dans la pratique, il peut s'agir de remplacer les données personnelles (nom, prénom, numéro personnel, numéro de téléphone, etc.) par des données d'identification indirecte (alias, numéro séquentiel, etc.) dans un ensemble de données, raisonnablement susceptible d'être utilisé.*

[2] *Le chiffrement garantit la confidentialité des données personnelles qui sont rendues illisibles sans clé de déchiffrement.*

en respectant les finalités du traitement de vos données personnelles.

Toutefois, si la Banque devait opérer un transfert de données personnelles au sein d'une entité du Groupe Santander qui se situe dans un pays en dehors de l'Union européenne n'assurant pas un niveau de protection adéquat, la Banque le ferait uniquement dans les cas prévus par la loi, par exemple en assurant la protection des données personnelles par des dispositions contractuelles adaptées.

Le transfert de vos données personnelles vers la base de données du Groupe Santander est effectué dans le but de répondre aux obligations légales. Notamment, le partage des données personnelles ainsi que de toute information pertinente liée aux transactions, permet aux Groupe Santander de se conformer à ses obligations légales relatives (i) à la réglementation anti-blanchiment et contre le financement du terrorisme ; (ii) au reporting réglementaire vis-à-vis des autorités de contrôle, et (iii) à la consolidation fiscale.

Les données personnelles qui sont partagées avec le Groupe Santander à ces fins sont les suivantes : vos données d'identification et des informations relatives à vos transactions.

## 8. Partenaires

Aucun transfert vers des tiers de vos données personnelles ne pourra être effectué, sans votre accord préalable, à des fins différentes que celles liées aux finalités du traitement de vos données par la Banque. Les seuls transferts qui sont effectués sont ceux auprès de la Banque Nationale Espagnole (conformément à la législation relative au Fonds de Garantie des dépôts), de la Cellule de Traitement des Informations Financières Belge (pour se conformer à la règlementation relative à la prévention du blanchiment de capitaux), du Service Public Fédéral Finance (pour se conformer aux règlementations FATCA et CRS) et du Groupe Santander (comme expliqué dans la section Groupe Santander ci-dessus).

La Banque conclut des contrats écrits avec ses sous-traitants qui contiennent au minimum les informations exigées par la législation et la réglementation en matière de protection des données et qui respectent la Politique de sous-traitance de la Banque. Les contrats prévoient expressément que le sous-traitant peut traiter les données personnelles exclusivement sur la base des instructions écrites de la Banque et cette dernière prévoit que le sous-traitant garantisse que les personnes en charge du traitement des données personnelles respectent la nature confidentielle de ces données. Les contrats prévoient aussi expressément si le sous-traitant est autorisé à travailler, à son tour, avec ses propres sous-traitants et les conditions qui doivent être respectées dans cette hypothèse.

**Sous-traitants au sein du Groupe Santander**

Pour le traitement de certaines données personnelles, la Banque utilise le Groupe Santander en tant que sous-traitant.

Certains traitements de données personnelles concernent des fonctions de supervision et de support (au niveau du groupe) telles que :

- Des services financiers;
- La fonction audit interne;
- Le support pour la facturation, les paiements et le traitement du crédit ;
- La technologie de l'information et autres services de logiciels bancaires ;
- Le marketing support.

**Sous-traitants du secteur financier**

La Banque utilise des tiers spécialisés en Belgique pour effectuer certaines opérations de traitement comme, par exemple, en ce qui concerne les paiements :

- SWIFT pour l'échange de messages à l'échelle mondiale ;
- Groupe ING pour les paiements et les transactions.

**Autres sous-traitants**

La Banque travaille avec des fournisseurs externes comme :

- Sopra Banking Software, entreprise de services du numérique, fournisseur de services technologiques ;
- Des sociétés pour les services de consultation et d'audit externe (comme par exemple PwC) ;
- Des entreprises spécialisées dans l'archivage et l'accès aux informations numériques telles qu'Iris Solutions SA, Systemat Digital Hub SA ou Iron Mountain ;
- Nordcall, pour notre service à la clientèle par lequel vous pouvez nous contacter ;
- We are Digital, Everis ou Maileon pour des services concernant la publicité.

## 9. Sécurité / confidentialité

La Banque s'engage à adopter les mesures techniques, physiques et organisationnelles adéquates pour protéger les données à caractère personnel contre l'accès non autorisé, le traitement illicite, la perte ou le dommage accidentels, et la destruction non autorisée.

### 9.1. Sécurité de l'équipement et de l'information

Toutes les données à caractère personnel électroniques détenues par la Banque sont conservées dans des systèmes protégés par des architectures de réseaux sécurisés avec des mises à jour périodiques, qui contiennent des firewalls et des modules de détection d'intrusion, afin d'empêcher les accès non autorisés aux données à caractère personnel par des tiers. Il existe une politique de "back up" de données sauvegardées sur les serveurs de manière à éviter les conséquences d'un effacement, d'une destruction ou d'une perte accidentelle. Les serveurs se trouvent dans des installations avec un haut degré de sécurité, dont l'accès aux personnes non autorisées est protégé via un système de détection d'incendie et d'autres systèmes réactifs.

### 9.2. Sécurité d'accès

L'importance de la sécurité de toutes les données à caractère personnel liées aux clients qui sont collectées, conservées et traitées dans le cadre de la gestion et de l'exécution de notre activité est une préoccupation majeure pour la Banque et le Groupe Santander. La Banque s'engage à protéger l'intégrité des informations personnelles et à empêcher l'accès non autorisé à celles-ci.

Des mesures sont conçues et prévues pour empêcher la corruption de données, pour bloquer l'accès inconnu et non autorisé à notre système informatique et à nos informations, et pour fournir une protection raisonnable des données à caractère personnel que la Banque possède. Tous les dossiers sont conservés confidentiellement dans des classeurs ou des pièces sécurisées et verrouillées. L'accès aux bases de données informatisées est contrôlé par une séquence login et requiert que les utilisateurs autorisés s'identifient eux-mêmes et fournissent un mot de passe avant que l'accès ne soit accordé. Les utilisateurs autorisés sont limités aux données nécessaires pour exercer leur fonction dans le cadre de la gestion et de l'exécution de notre activité.

Les caractéristiques de sécurité des softwares et des procédures développées sont utilisées pour

protéger les informations personnelles de perte, d'abus, et d'accès non autorisé, de divulgation, d'altération, et de destruction.

### 9.3. Formation

La Banque organise des sessions de formation nécessaires pour les utilisateurs autorisés à propos notamment des finalités licites, énumérées et prévues pour le traitement de données à caractère personnel, du besoin de protéger et de garder l'information exacte et à jour, des finalités licites pour la collecte, et du besoin de maintenir la confidentialité des données auxquelles les utilisateurs autorisés ont accès.

Les utilisateurs autorisés s'engageront à respecter la confidentialité des données à caractère personnel et à se conformer à la présente Politique. La Banque prendra les mesures nécessaires conformément à la législation et à la réglementation en matière de protection des

données, si l'on accède à des données à caractère personnel, ou si celles-ci sont traitées ou utilisées de manière non conforme aux exigences de la présente Politique.

### 9.4. Instructions générales

Tous les utilisateurs autorisés sont tenus, en vertu de la présente Politique, de faire le nécessaire pour respecter les règles établies dans la présente Politique afin que la Banque, en tant que responsable du traitement, respecte la législation et la réglementation en matière de protection des données. La Banque s'engage à protéger les données à caractère personnel du client lors de leur utilisation ou de leur traitement. C'est pourquoi les utilisateurs autorisés doivent reconnaître l'importance d'un traitement correct et licite des données à caractère personnel et doivent gérer les données à caractère personnel avec le plus grand soin et ce, conformément à la présente Politique.

### 9.5. Incidents de sécurité

Par un incident de sécurité qui affecte les données personnelles, la Banque entend :

- L'accès, la communication et /ou l'utilisation non autorisée de vos données personnelles ;
- La modification, la destruction, la perte ou l'altération accidentelle ou illicite de vos données personnelles transmises, stockées ou traitées par une ou plusieurs personne(s) sans autorisation ;
- L'impossibilité d'accéder à vos données personnelles.

Les entités financières sont confrontées tous les jours à des menaces susceptibles de nuire à l'intégrité et à la confidentialité de vos données personnelles.

Il importe de souligner que seules les personnes autorisées ont accès à vos données personnelles et que celles-ci sont stockées sur un nombre limité de serveurs. La Banque et ses sous-traitants ne disposent que des données personnelles nécessaires à la réalisation de leurs tâches.

La Banque a mis en place des outils et des procédures d'intervention en cas de violation de la sécurité de ses systèmes, pouvant causer la destruction accidentelle ou illicite, la perte, la modification, la divulgation non autorisée ou l'accès par des personnes non-autorisées aux données personnelles, transmises, stockées ou traitées différemment.

Dans le cas d'une fuite de données personnelles, la Banque en informeraà l'Agence de Protection des Données en Espagne, et si necessaire, vous tiendra également informé.

La Banque fait partie du Groupe Santander, un des plus grands groupes financiers du monde. La

cybersécurité est l'une de ses principales préoccupations.

La Banque a pour vocation de travailler en partenariat avec tous les secteurs du Groupe Santander pour protéger les clients et leurs données personnelles ainsi que les employés et les systèmes contre les menaces actuelles et imminentes en matière de cybersécurité.

## 10. Période de rétention de vos données

Les informations à caractère personnel, que vous transmettez volontairement lorsque vous sollicitez un de nos services et les informations collectées au cours de la relation contractuelle sont conservées par la Banque pendant la durée nécessaire à la réalisation des finalités poursuivies pour leur traitement ou pendant la durée imposée par la loi en vigueur (voir Collecte de vos données à caractère personnel et finalités des traitements).

À la fin de la relation contractuelle, vos données seront encryptées et supprimées. Pour des obligations comptables, l'encryptage sera effectué un an après la fin de la relation contractuelle et la suppression sera effectuée 10 ans après la fin de la relation contractuelle pour vos données d'identification et 10 ans après le dernier mouvement de compte pour les informations relatives à vos transactions, comme prévu par la loi relative à la prévention du blanchiment de capitaux. La loi oblige à sauvegarder les données des prospects qui ont sollicité une ouverture de compte mais qui n'ont jamais activé leur compte (à savoir, n'ont jamais finalisé le processus). La période de rétention pour ces données est le même que pour les clients activés.

Après la fin de la relation contractuelle, vos données personnelles pourraient seulement être utilisées pour des raisons légales.

Si vous avez accepté de recevoir de la publicité et que vous n'avez pas exercé votre droit à l'oubli, la Banque garde vos coordonnées afin de pouvoir continuer à vous envoyer de la publicité. Si vous voulez retirer votre consentement, il vous suffit d'envoyer un e-mail à dataprotection@santanderconsumerbank.be . Sur simple demande, vos données personnelles seront supprimées et les données restantes seront utilisées à des fins statistiques (données agrégées anonymisées, c'est-à-dire analysées globalement pour en faire un résumé anonymisé).

Pour les personnes qui ont initié une ouverture de compte sans avoir finalisé l'étape 2 (données de mon compte) et qui ont accepté de recevoir de l'aide pour continuer le processus d'ouverture de compte, toutes les informations fournies seront stockées pendant 30 jours et, après cette période, les données personnelles seront supprimées et les données restantes seront utilisées à des fins statistiques (données agrégées anonymisées, c'est-à-dire analysées globalement pour en faire un résumé anonymisé).
Si vous n'avez pas accepté de recevoir de la publicité, aucune donnée personnelle ne sera enregistrée.

Dans certains cas, la Banque peut cependant refuser d'effacer ces données, par exemple pour l'introduction, la mise en œuvre ou la preuve d'un droit en justice.

## 11. Protection et confidentialité

Seules les personnes qui y sont habilitées ont accès aux données à caractère personnel qui sont pertinentes pour l'accomplissement de leur mission. Ces personnes ne peuvent utiliser ces données personnelles que si elles sont nécessaires à l'accomplissement de leur mission. Elles sont tenues de respecter une stricte discrétion professionnelle et toutes les prescriptions techniques tendant à la préservation de la confidentialité des données à caractère personnel et à la sécurité des systèmes qui les contiennent.

La Banque prend des mesures techniques et organisationnelles en interne pour éviter que les données à caractère personnel ne tombent entre les mains de personnes non autorisées ou qu'elles ne soient modifiées ou détruites par inadvertance. Les locaux, les serveurs, le réseau, les transferts et les données personnelles sont protégés en application de règles internes. Le contrôle de ces protections

sera à son tour effectué par un service spécialisé.

## 12. Exercice de vos droits

Lors du traitement de vos données à caractère personnel par la Banque, vous avez les droits suivants :

- Le droit d'accès à vos données personnelles ;
- Le cas échéant, le droit à la rectification de données personnelles non-correctes ;
- Le droit d'opposition au traitement de vos données personnelles et le droit à l'oubli ;
- Le droit à la portabilité de vos données personnelles.

**Le droit d'accès**

Le droit d'accès vous donne le droit d'obtenir gratuitement :

- La confirmation que vos données à caractère personnel sont traitées, les informations portant sur la finalité du traitement, les catégories de données personnelles traitées et les catégories de destinataires ;
- La communication, sous une forme compréhensible, des données personnelles traitées et de toute information disponible sur leur origine ;
- Les informations disponibles sur l'origine des données personnelles ainsi que les communications effectuées ou à venir.

**Le droit de rectification**

Le droit de rectification vous donne le droit d'obtenir sans frais la rectification de toute donnée à caractère personnel inexacte qui vous concerne.

Le traitement de la demande consistera essentiellement en la rectification de vos données personnelles ou en un refus d'accéder à cette demande dans les cas prévus par la législation belge ou européenne en vigueur.

**Le droit d'opposition et le droit à l'oubli**

Le droit d'opposition vous donne le droit de vous opposer gratuitement à ce que les données personnelles vous concernant fassent l'objet d'un traitement, par exemple à des fins de prospection commerciale.

Le droit à l'oubli consiste à obtenir de la Banque l'effacement des données personnelles vous concernant, en tenant compte de la période de conservation appliquée.

Le droit d'opposition n'est pas admis pour les traitements nécessaires à la conclusion ou à l'exécution du contrat d'ouverture de compte ou pour les traitements imposés par une obligation légale ou réglementaire.

Dans le cadre du droit d'opposition, lorsque vos données personnelles ont été collectées à des fins de marketing direct, vos données personnelles seront supprimées et les données restantes seront utilisées à des fins statistiques (données agrégées anonymisées, c'est-à-dire analysées globalement pour en faire un résumé anonymisé).

Pour plus d'informations concernant le droit à l'oubli, veuillez consulter Période de rétention de vos données personnelles.

**Le droit à la portabilité**

Vous avez le droit de recevoir les données personnelles vous concernant, celles que vous avez fournies à la Banque, dans un format structuré, communément utilisé et lisible par machine. Vous pouvez également demander à la Banque de les transmettre à un tiers.

## 13. Comment exercer vos droits ?

La demande peut être adressée à la Banque :

- Via l'adresse électronique de contact mailto:dataprotection@santanderconsumerbank.be;
- En appelant notre service à la clientèle ;
- Par courrier postal à l'adresse suivante :

Santander Consumer Finance, S.A. - succursale en Belgique
Guldensporenpark 81
9820 Merelbeke, Belgique.

Santander Consumer Finance, S.A. - Monte
Avenida de Cantabria s/n.
28660 Boadilla del Monte, España.

Toutes les réponses sont envoyées dans votre espace personnel sécurisé pour des raisons de sécurité et d'identification. Si vous désirez recevoir une réponse par un autre moyen de communication, vous devez envoyer à la Banque une copie recto-verso de votre carte d'identité. En cas de difficultés rencontrées dans l'exercice de vos droits consacrés par la loi ou en cas de non-respect d'obligations découlant de la loi, vous pouvez adresser une plainte à la Banque, à l'adresse suivante :

plaintes@santanderconsumerbank.be
klachten@santanderconsumerbank.be

La Banque fournit au client des informations sur les mesures prises à la suite d'une demande formulée en application de ces clauses, dans les meilleurs délais et en tout état de cause dans un délai d'un mois à compter de la réception de la demande. Si nécessaire, ce délai peut être prolongé de deux mois, compte tenu de la complexité et du nombre de demandes. La Banque informera le client de cette prolongation, et des motifs de celle-ci, dans un délai d'un mois à compter de la réception de la demande.