MIGROSBANK

Déclaration de confidentialité relative aux applications d'e-banking de la Banque Migros

1 Généralités

La Banque Migros SA («Banque Migros», «nous») propose un accès sûr à ses prestations d'e-banking via Internet grâce à ses applications d'e-banking pour smartphone, tablettes et PC («application» ou «application d'e-banking»).

La Banque Migros accorde une grande importance à la protection des données personnelles et respecte scrupuleusement les dispositions des lois suisses sur la protection des données. Les informations ci-après offrent un aperçu des données relevées par l'application et des objectifs poursuivis.

2 Quelles sont les données personnelles relevées?

Tant que l'application d'e-banking n'est pas activée par la saisie du numéro de contrat EB et du code d'activation, l'application peut être utilisée sans entrer de données personnelles.

Lors de l'activation de l'application, le système sollicite les données supplémentaires suivantes dans le but d'identifier le client ainsi que de lier l'application à l'appareil utilisé et à votre contrat d'e-banking:

- Numéro de contrat d'e-banking
- Code d'activation à usage unique
- Mot de passe

D'autres données techniques sont automatiquement relevées en arrière-plan:

- Propriétés de l'appareil utilisé (type d'appareil et fabricant, système d'exploitation utilisé et version, ID de l'appareil, adresse IP, taille de l'écran, langue sélectionnée)
- Version de l'application d'e-banking

L'utilisation des prestations d'e-banking après activation repose sur les «conditions d'utilisation des prestations d'e-banking» acceptées par le client.

3 Quels sont les droits système nécessaires à l'application?

L'utilisation de l'application requiert des droits garantissant son fonctionnement et sa sécurité. Ces droits varient en fonction de la plate-forme (smartphone, tablette, PC) et du système d'exploitation (Android, iOS, Windows, macOS).

Les droits pouvant être sollicités sont les suivants:

- Accès à la caméra (uniquement pour smartphone): ce droit est nécessaire à la lecture de bulletins de versement et de codes-barres. Les images ne sont ni enregistrées ni transmises.
- Accès à la mémoire et aux données (lecture, modification, suppression): pour que l'application puisse enregistrer et lire localement des données propres, les droits correspondants doivent être demandés.
- Accès à Internet: l'accès à Internet est nécessaire pour que l'application puisse échanger des données avec les serveurs de la Banque Migros.
- Lecture de contacts (uniquement pour smartphone): ce droit est utilisé exclusivement par la fonction «MobilPay P2P» afin de sélectionner des contacts locaux du carnet d'adresses aux fins de virements.
- Recherche de comptes: ce droit est nécessaire à l'établissement de rapports de défaillances. Cette option est désactivée par défaut et peut être activée manuellement par l'utilisateur en cas de besoin.
- Afficher via d'autres applications: sert uniquement à l'affichage protégé de données de transactions.

- Désactiver le mode veille (tablette) ou déverrouiller l'écran (smartphone), commander le vibreur: ces droits sont nécessaires pour signer des paiements.
- Accès au capteur d'empreinte digitale (smartphone uniquement): si votre appareil dispose d'un capteur d'empreinte digitale, vous pouvez l'utiliser pour l'e-banking. Cette autorisation est requise à cet effet.

Pour des raisons de sécurité, des droits supplémentaires sont également nécessaires dans le but de fixer l'application sur un appareil unique. L'application utilise un identifiant d'appareil univoque afin d'éviter toute copie (à cette fin, l'autorisation de «lire l'état du téléphone et l'identité», notamment, est requise).

À titre de dispositif d'autoprotection, l'application utilise par ailleurs des fonctions de sécurité permettant, par exemple, d'identifier les applications et paramètres (ex. «Jailbreaks») potentiellement dangereux pour la sécurité de l'accès à l'e-banking (le droit «Appeler des applis actives», par exemple, est nécessaire).

Si le «Mobile Widget» est utilisé sur un smartphone Android, cette fonction nécessite les droits de création et de gestion d'un compte local et des paramètres de synchronisation correspondants.

Si l'utilisateur se procure un appareil de remplacement (Air+) auprès de la Banque Migros et souhaite l'utiliser avec un smartphone ou une tablette, les autorisations Bluetooth nécessaires au raccordement et à l'utilisation de l'appareil de remplacement sont indispensables. Pour ce faire, Android doit avoir accès au site géographique approximatif.

Si l'utilisateur a autorisé son navigateur Web à utiliser des données géographiques, la recherche de succursales et DAB peut exploiter sa position actuelle pour faciliter le processus de recherche. Les informations relatives à l'emplacement ne sont pas enregistrées.

Si l'utilisateur n'a pas besoin de certaines fonctions, il peut en supprimer les droits (p. ex. pour la caméra, les contacts, Bluetooth ou la position géographique). Les possibilités en la matière dépendent du système d'exploitation utilisé.

4 Comment les données du client sont-elles protégées?

Pour assurer la protection des données, nous utilisons, entre autres, les dispositifs de sécurité suivants:

- Sur l'appareil de l'utilisateur: les rapports de défaillances et les données sensibles sont encodées puis archivées localement par l'application.
- Lors de la transmission: l'application communique par relations codées et sécurisées.
- À la Banque Migros: nous protégeons les données de l'utilisateur grâce à des mesures organisationnelles et techniques contre l'accès non autorisé ou illicite, la modification ou l'abus. Toutes les données sont enregistrées en Suisse.

L'application communique par le biais d'un réseau public (Internet). Même si l'utilisateur se connecte en Suisse, il est possible que les données soient transmises vers l'étranger. Bien que l'application communique par codes, l'émetteur et le récepteur des paquets de données peuvent être identifiés. La communication entre l'utilisateur et la Banque peut donc être retracée.

5 Notifications par e-mail et SMS

L'envoi de notifications par e-mail et SMS depuis l'e-banking n'est pas crypté; les données peuvent donc être interceptées et consultées par des tiers. La Banque Migros SA apparaît en tant qu'expéditrice, ce qui permet à des tiers d'identifier votre relation bancaire avec nous. Par conséquent, le secret bancaire n'est pas garanti lors de l'activation des notifications par e-mail et SMS.

6 E-facture et eBill

L'utilisation des fonctions «E-facture» et «eBill» est soumise aux dispositions de protection des données du prestataire SIX Paynet SA. Celles-ci peuvent être consultées sur https://www.e-facture.ch/Conditions-dutilisation.html ou https://ebill.ch/fr/declaration-de-confidentialite.

7 Comment utilisons-nous les fichiers d'historique?

Afin de garantir une exploitation sûre et correcte et de pouvoir analyser les erreurs, les accès à nos prestations d'e-banking depuis l'application sont documentés dans des fichiers d'historique sur nos serveurs.

8 L'application recueille-t-elle des données sur le comportement des utilisateurs?

Pour pouvoir améliorer et optimiser l'application sur une base continue, nous recueillons des informations anonymes sur l'utilisation de l'application et de ses fonctions. Ces données ne sont pas exploitées aux fins d'identification du client. De même, l'application ne fait appel à aucun prestataire externe pour le prélèvement et l'évaluation de ces données.

9 Quelles sont les données transmises à des tiers?

L'application ne transmet aucune donnée personnelle à de tierces parties. Les éventuelles requêtes effectuées auprès de partenaires externes pour le compte de l'utilisateur (p. ex. cours boursiers) se font sur une base anonyme ne permettant aucune identification du requérant.

Lors du téléchargement de l'application depuis un App Store et de l'utilisation de l'application, il se peut que les fabricants d'appareils ou de systèmes d'exploitation (p. ex. Microsoft, Apple ou Google) reçoivent des données personnelles ou analysent le comportement de l'utilisateur, et puissent ainsi établir un lien entre vous-même et la Banque Migros. Nous ne pouvons empêcher ni influencer cette éventualité.

10 Comment supprimer les données de l'application?

La désinstallation de l'application entraîne la suppression de toutes les données créées localement par l'application. Vous pouvez supprimer à tout moment les appareils activés dans votre e-banking.

11 Modification de la déclaration relative à la protection des données

La présente déclaration peut être adaptée aux besoins. Nous actualiserons dès lors le numéro de version et la date du document, et publierons la nouvelle version dans l'application ainsi que sur notre site Internet.

12 Complément d'informations

Vous avez le droit de demander des renseignements sur les données personnelles mémorisées, de les faire rectifier ou de refuser leur utilisation à des fins de marketing. Vous pouvez également exiger leur suppression, pour autant que nous ne soyons pas tenus de les conserver de par la loi ou pour des motifs réglementaires. Vous pouvez envoyer une demande de renseignements par courrier recommandé avec copie d'une pièce d'identité à l'adresse ci-dessous.

Veuillez nous contacter comme suit si vous avez des questions au sujet du traitement de vos données personnelles ou de cette déclaration de confidentialité:

Banque Migros SA
Protection des données
Case postale
8010 Zurich

info@migrosbank.ch

Version 1.2 du 18.05.2018