Banque et trafic des paiements

Mise à jour de l'édition 2023 – juin 2024

GENEHMIGT

Swiss Banking

compendio
Bildungsmedien

www.compendio.ch/bankingtoday
www.cyp.ch
www.swissbanking.org

Banque et trafic des paiements
Mise à jour de l'édition 2023 – juin 2024

Relecture: Comité d'experts médias didactiques Swiss Banking
Conception graphique et mise en page: icona basel gmbh
Réalisation et révision: Compendio Bildungsmedien AG, Zurich
Illustrations: Valentina Morrone, www.valentinamo.ch
Impression: Edubook AG, Merenschwand

Conception: groupe de travail du CYP dirigé par Alexia Böniger, Thomas Hirt, Compendio Bildungsmedien AG,
et Cyril Locher, Crealogix
Réalisation: Christoph Gütersloh et Thomas Hirt, Compendio Bildungsmedien AG
Suivi éditorial avec mises à jour: Remy Gerspacher, Compendio Bildungsmedien AG et al.

Numéro d'article: Update
Édition: 1e édition
Dépôt légal: 01N24
Langue: FR
CYP

Réalisée en Suisse, l'impression de cet ouvrage est climatiquement neutre. La société Edubook AG a fait l'objet d'un audit climatique visant en priorité à réduire et à éviter les émissions de CO_2. Elle compense ses rejets résiduels en achetant des certificats CO_2 issus d'un projet suisse de protection du climat.

Corrections et ajouts (juin 2024)

Le secteur bancaire se trouvant en constante évolution, le contenu de la formation Banking-Today est appelé à être mis à jour d'année en année. Il est en effet essentiel pour nous de proposer des supports didactiques à la pointe de l'actualité.

C'est pourquoi Compendio Bildungsmedien fait paraître chaque année une version actualisée et corrigée de BankingToday.

La présente mise à jour doit permettre aux personnes ayant acheté l'édition 2023 de disposer elles aussi d'informations aussi récentes que possible:

- Cette mise à jour sera complétée début juin pendant trois années consécutives et publiée sur le site **www.compendio.ch/bankingtoday**.
- Ce système permet de garantir la connaissance de l'ensemble des modifications et des ajouts au matériel didactique en vue de la phase de préparation des examens finaux au printemps ou en été.

Conseil: Nous vous recommandons de prendre connaissance le plus tôt possible dans la phase de préparation des changements et des compléments apportés, et de les reporter sans attendre dans le matériel didactique. Vous aurez ainsi un premier aperçu de ces modifications et les assimilerez plus facilement.

<table>
<tr><th>Section</th><th>La banque 1 – Introduction à l'univers bancaire</th></tr>
<tr><td>Chapitre 1</td><td>Pas de corrections.</td></tr>
<tr><td>2.1.2 Information complémentaire: Les catégories de banques dans les statistiques de la Banque nationale suisse</td><td>Après la reprise de la CS par l'UBS, il n'y a plus qu'une seule grande banque en Suisse.
Grandes banques
UBS SA est désormais la seule grande banque de la Suisse.

<table>
<tr><td>Clientèle/ activité commerciale</td><td>UBS est une banque universelle. Elle compte parmi les plus grandes du monde dans les domaines de la banque privée et de la banque d'investissement.</td></tr>
<tr><td>Rayon géographique</td><td>Malgré sa forte orientation internationale, UBS est également très active en Suisse et largement représentée par des succursales bancaires en Suisse.</td></tr>
<tr><td>Forme juridique</td><td>UBS est une société anonyme.</td></tr>
<tr><td>Particularités</td><td>La somme du bilan de UBS représente une part importante du total du bilan de toutes les banques suisses. Afin de garantir la confidentialité des données, la BNS ne publie plus de chiffres détaillés sur le groupe bancaire des grandes banques.</td></tr>
</table></td></tr>
<tr><td>Chapitre 3 + 4</td><td>Pas de corrections.</td></tr>
</table>

Section	La banque 2 – Réglementation bancaire, compliance, comptes annuels et gestion des risques
1.3.1. Informations complémentaires concernant la nouvelle loi sur la protection des données (nLPD)	La protection des données n'a cessé de gagner en importance ces dernières années. Des données susceptibles d'être **crées, exploitées, analysées, enregistrées** mais aussi **utilisées abusivement** sont aujourd'hui disponibles en très grandes quantités. Dans le secteur bancaire en particulier, où des données personnelles sont crées puis utilisées, la protection des données est généralement primordiale, outre le secret bancaire, par exemple: • lors de l 'établissement de nouvelles relations d'affaires avec des clients privés (personnes physiques), • lors du recrutement de nouveaux collaborateurs et collaboratrices, • dans le cadre d 'affaires avec des concurrents dans lesquelles des données personnelles, par exemple concernant leur personnel, sont traitées, ou encore, • lors de la collecte de données personnelles à des fins de marketing. **Quels sont les fondements juridiques?** La LPD entièrement révisée est entrée en vigueur le 1er septembre 2023 et s 'applique à l 'ensemble des entreprises et des secteurs qui traitent les données personnelles de personnes physiques, c 'est-à-dire qui collectent, enregistrent, conservent, utilisent, modifient, communiquent, archivent, suppriment, etc. des données personnelles. Selon le modèle commercial et le cas d 'utilisation, il est possible que le RGPD UE soit applicable en plus de la LPLD, et ce également pour les entreprises ayant leur siège en Suisse. Le champ d'application territorial du RGPD pour les responsables du traitement non établis dans l 'UE découle de l 'article 3, paragraphe 2 du RGPD UE. Le règlement ne s'applique donc pas uniquement aux personnes physiques, domiciliées dans l 'UE. Le présent règlement s'applique au traitement des données à caractère personnel des personnes concernées se trouvant dans l 'UE par un responsable non établi dans l 'UE si le traitement des données est lié au fait a) de proposer des biens ou de services aux personnes concernées dans l'UE ou l 'EEE, indépendamment de l 'obligation ou non d 'effectuer un paiement par ces personnes concernées; b) de surveiller le comportement des personnes concernées dans la mesure où leur comportement a lieu au sein de l'UE ou l 'EEE. La protection des données est étroitement liée au secret bancaire (art. 47 LB; cf. module «La banque 1»), même si leurs objectifs sont différents. Le secret bancaire s 'étend aux personnes physiques et aux personnes morales et protège la confidentialité des clients et clientes de la banque, p. ex. contre la remise des données à de véritables tiers, tandis que la LPD s 'applique aux personnes physiques et vise avant tout à protéger l 'autodétermination en matière d 'information. **Objectifs de la nouvelle loi sur la protection des données entièrement révisée** La loi sur la protection des données ne vise pas à protéger les données personnelles, mais l 'autodétermination en matière d 'information de la personne à laquelle les données personnelles se rapportent. Quiconque traite des données personnelles doit donc respecter ce que l 'on appelle les principes de traitement et satisfaire aux obligations légales. La surveillance de la protection des données relève de la compétence du Préposé fédéral à la protection des données et à la transparence **(PFPDT).** **Qui peut invoquer la protection des données et quelles sont les données concernées?** Le droit en matière de protection des données protège les personnes physiques dont les données personnelles font l'objet d'un traitement: • Par **données personnelles,** on entend toutes les informations qui se rapportent à une personne physique (p. ex. le numéro de téléphone, une photo, une adresse e-mail, le numéro de sécurité sociale ou l'adresse IP). • Les données sensibles sont des données personnelles de la **sphère secrète et privée.** Il s'agit notamment de données sur les opinions ou activités religieuses, politiques ou syndicales, sur la santé ou sur des poursuites et sanctions pénales. Leur traitement doit faire l'objet d'une attention particulière.

Section	La banque 2 – Réglementation bancaire, compliance, comptes annuels et gestion des risques	
	Quels sont les principes à respecter dans le traitement des données personnelles? Tout traitement de données personnelles doit être licite. Cela signifie qu'il ne faut pas enfreindre la loi et que le traitement des données ne doit pas porter atteinte de manière illicite à la personnalité de la personne physique. Les principes suivants doivent être respectés lors du traitement des données: **Fig. 1-7** Principes du traitement des données (se reporter à l'art. 6 LPD)	
	Légalité, proportionnalité et bonne foie	Le traitement des données personnelles est **proportionnel** s 'il est approprié pour atteindre l 'objectif poursuivi. Pour cela, les données à traiter doivent être nécessaires. En règle générale, il est possible d 'utiliser plus de données personnelles lorsqu 'un traitement de données poursuit plusieurs finalités. Les données personnelles sont détruites ou anonymisées dès qu 'elles ne sont plus nécessaires aux fins du traitement - les obligations d 'archivage légales ou privées demeurent réservées.
	Affectation à un but précis et transparence	Les données personnelles ne peuvent être collectées que dans une **finalité précise** et identifiable par la personne concernée; elles ne peuvent être traitées que de manière compatible avec cette finalité.
	Intégrité des données (exactitude)	Quiconque traite des données personnelles doit s'assurer de leurs **exactitude.** Cela suppose que l 'on ait défini pour chaque cas d 'utilisation les exigences en matière d 'exactitude. Elle ou il doit prendre toutes les mesures appropriées pour que soient rectifiées, effacées ou détruites les données qui sont inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées.
	Consentement	Lorsque, à titre exceptionnel, le **consentement** de la personne concernée est requis, ce consentement n'est valable que s'il est accordé librement pour un ou plusieurs traitements déterminés, après que la personne a été dûment informée. Si un consentement est requis à titre exceptionnel, il doit être explicite pour les traitements de données suivants: a) le traitement de données personnelles particulièrement sensibles; b) un profilage à haut risque effectué par une personne privée; ou c) un profilage effectué par un organe fédéral; d) une divulgation dans un État étranger ne disposant pas d 'un niveau de protection des données approprié.
	Fig. 1-8 Obligations lors du traitement des données	
	Obligation d'information	Lorsque des données personnelles sont collectées, la personne concernée doit en être **informée,** sauf exceptions prévues à l 'article 20 LPD. La personne concernée doit connaître l'identité et les coordonnées du responsable du traitement ainsi que la finalité du traitement. Si les données personnelles sont transmises à des tiers à des fins de traitement, ceux-ci doivent également être communiqués. Si les données personnelles de la personne concernée ne sont pas collectées auprès de celle-ci, les catégories de données personnelles traitées doivent en outre être communiquées à la personne concernée (cf. art. 19, al. 3 LPD). Si les données personnelles sont communiquées à l'étranger, l'État ou l'organe international auquel elles sont communiquées doit également être communiqué à la personne concernée (cf. art. 19, al. 4 LPD).

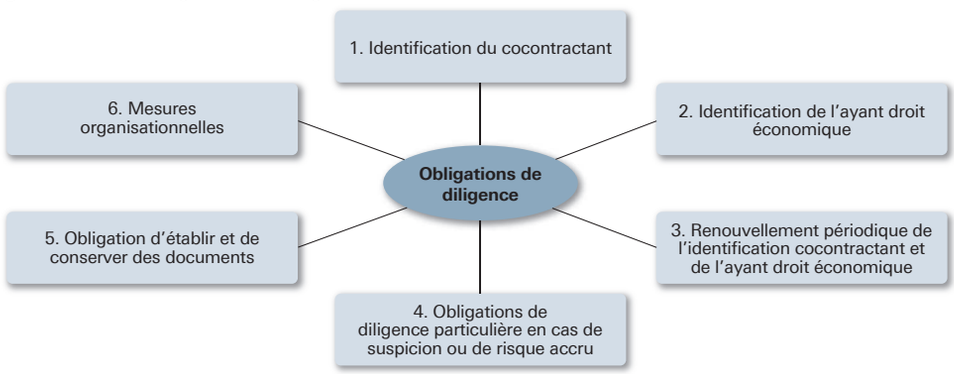
Section	La banque 2 – Réglementation bancaire, compliance, comptes annuels et gestion des risques	
	Obligation de tenir un registre	Le responsable du traitement et le sous-traitant doivent tenir chacun un **registre de leurs activités de traitement** (cf. art. 12, al. 1 LPD). **ATTENTION:** ILe Conseil fédéral prévoit des exceptions pour les entreprises employant moins de 250 collaborateurs et collaboratrices et dont le traitement des données présente un risque limité d'atteinte à la personnalité des personnes concernées (cf. art. 12, al. 5 LPD). • l'identité du responsable du traitement; • la finalité du traitement; • une description des catégories de personnes concernées et des catégories de données personnelles traitées; • les catégories des destinataires; • dans la mesure du possible, la durée de conservation des données personnelles ou les critères permettant de définir cette durée; • dans la mesure du possible, une description générale des mesures permettant de garantir la sécurité des données; • si les données sont communiquées à l'étranger, le nom de l'État concerné ainsi que les garanties.
	Obligation d'annonce	S'il y a violation de la sécurité des données (« data breach ») et que celle-ci entraîne vraisemblablement un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, il convient de **signaler** cette violation le plus rapidement possible. Le responsable du traitement signale au **PFPDT** (Préposé fédéral à la protection des données et à la transparence) dans les meilleures délais toute violation de la sécurité des données susceptible d'engendrer un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. Dans son signalement, il ou elle mentionne au moins la nature de la violation de la sécurité des données, ses conséquences et les mesures prises ou prévues (cf. art. 6, al. 1 et 2 LPD). Le sous-traitant rapporte dans les meilleurs délais toute violation de la sécurité des données au responsable du traitement. Si cela est nécessaire à la protection de la personne concernée ou si le PFPDT le demande, le responsable du traitement informe la personne concernée (cf. art. 6, al. 3 et 4 LPD).
	Analyse d'impact relative à la protection des données personnelles	En raison de la rapidité des évolutions technologiques, les conséquences d'un traitement des données sont parfois difficiles à prévoir. Il convient donc d'effectuer une **analyse d'impact relative à la protection des données personnelles** (AIPD) si un traitement est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées. L'analyse d'impact comprend une description du traitement prévu. Elle doit indiquer les risques liés au traitement des données et les mesures de protection de la personnalité et, le cas échéant, des droits fondamentaux (cf. art. 22, al. 3 LPD). **ATTENTION:** L'analyse d'impact relative à la protection des données doit être établie **au préalable.**
	«Privacy by Design» et «Privacy by Default»	Le responsable du traitement est tenu de garantir la protection des données via la technologie - ce que l'on appelle **«Privacy by Design»**, et via la protection des données par défaut - ce que l 'on appelle **«Privacy by Default».** Dans ce cadre, les prescriptions légales sont traduites, par les services spécialisés et les fonctions qui en ont la compétence, en prescriptions autonomes pour les mesures techniques et organisationnelles (MTO) (cf. art. 7 LPD).

Section	La banque 2 – Réglementation bancaire, compliance, comptes annuels et gestion des risques	
	Transfert de données à des tiers et transmission à l'étranger	Lorsque des données personnelles sont transmises ou qu'elles sont transférées à l'étranger, on perd dans une certaine mesure le contrôle de ces données. Il existe un risque que les données personnelles ne bénéficient pas d 'une protection appropriée, c 'est-à-dire notamment que les principes de traitement (voir ci-dessus) ne puissent être respectés, et que les droits des personnes concernées soient ainsi bafoués. C 'est pourquoi des règles particulières s 'appliquent pour le transfert de données et la transmission à l 'étranger. **Transfert de données à des tiers:** Les données personnelles peuvent être transmises à des sous-traitants (cf. art. 5 let. k et 9 LPD), si cela est convenu par contrat ou prévu par une loi et que la sécurité des données est garantie. **Transmission de données à l'étranger:** Les données personnelles peuvent être communiquées sans conditions supplémentaires aux pays qui garantissent un niveau de protection des données adéquat (cf. art. 16 LPD). Le Conseil fédéral définit les pays disposant d'une protection «appropriée». Il publie une liste de ces pays. Par exemple, tous les États membres de l'UE offrent une protection appropriée.
	Profilage et décisions individuelles automatisées	Le **profilage** est toute forme de traitement automatisé de données personnelles consistant à utiliser ces données personnelles pour mettre en évidence certains aspects personnels relatifs à une personne physique, pour analyser ou prédire des aspects concernant la performance au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, le lieu de séjour ou de déplacement de cette personne physique (art. 5, let. f LPD). Exemple: Création automatisée d 'un profil client pour la diffusion de publicités en ligne sur mesure ou pour soumettre des recommandations de placement appropriées. Une **décision individuelle automatisée** est une décision qui repose exclusivement sur un traitement automatisé et qui entraîne pour celui-ci des conséquences juridiques ou l 'affecte de manière significative (art. 21 LPD). Exemple: Évaluations automatisées de la solvabilité pour accepter et exécuter automatiquement les ordres d 'un client dans l 'e-banking.
	Quel droit une personne a-t-elle sur ses données? Les personnes concernées par un traitement des données disposent notamment des droits suivants: **Fig. 1-9** Droits d'une personne concernée par un traitement de données	
	Droits des personnes concernées	**Droit d'accès:** En règle générale, les personnes concernées ont le droit d 'obtenir des renseignements sur les informations suivantes (cf. art. 26 LPD concernant la limitation, l 'ajournement et le refus du droit d 'accès): • Identité / coordonnées du responsable du traitement • Données personnelles traitées • Finalité du traitement • Durée de conservation • Origine des données personnelles traitées • S'agit-il d'une décision individuelle automatisée? • Destinataires tiers de données personnelles traitées Le responsable du traitement doit fournir des informations gratuitement, généralement dans un délai de 30 jours.
	Droit à la portabilité des données	Toute personne peut exiger du responsable du traitement la **divulgation de ses données personnelles électroniques** si celui-ci traite les données de manière automatisée et si les données personnelles ont été traitées avec le consentement de la personne ou en relation avec un contrat (cf. art. 28, al. 1 LPD).

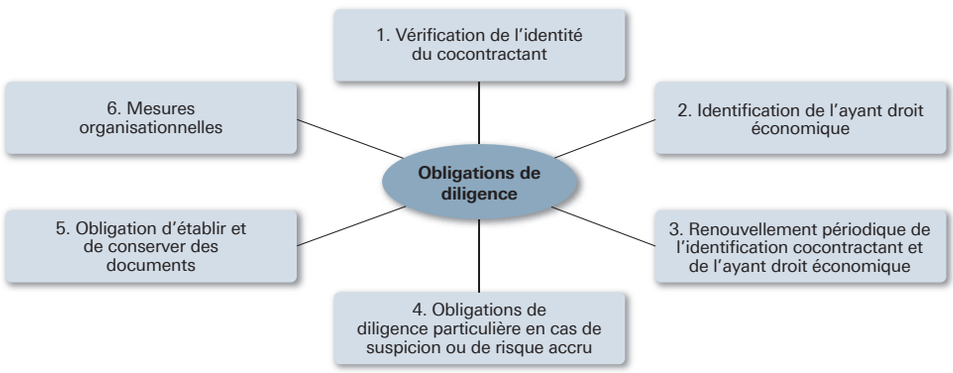
Section	La banque 2 – Réglementation bancaire, compliance, comptes annuels et gestion des risques	
	Droit de rectification et droit à «l'oubli»	Lorsque des données personnelles sont inexactes, il existe un **droit de rectification.** La personne concernée peut exiger une telle rectification, à moins qu'une disposition légale ne l'interdise ou que les données personnelles ne soient traitées à des fins d'archivage d'intérêt public. Il en va même pour le **droit à l 'effacement** ou à **l ' «oubli»:** Lorsque la finalité d 'un traitement de données personnelles est atteinte et qu 'il n 'existe aucun motif d 'archivage légal ou privé, leur suppression peut être exigée.
	Quand y a-t-il violation des dispositions en matière de protection des données? Si, en particulier, les principes de traitement des données ne sont pas respectés et qu 'il n 'existe pas de motif justificatif, il y a généralement violation de la protection des données, c 'est-à-dire infraction à la loi sur la protection des données (LPD). Les **motifs de justification** possibles sont: • le consentement de la personne concernée, • une autorisation légale ou • un intérêt prépondérant privé et / ou public.	
	Exemple Il y a par exemple violation de la protection des données lorsqu 'une banque utilise des adresses accessibles au public à des fins publicitaires et n 'en a pas informé la personne concernée (p.ex., la banque a omis de fournir aux personnes concernées un lien vers la déclaration de protection des données dans la brochure publicitaire). **Comment une personne peut-elle se défendre en cas de violation de la loi sur la protection des données?** La personne concernée peut notamment demander l'interdiction d'un traitement déterminé de données personnelles, l'interdiction d'une communication déterminée de données personnelles à des tiers, ainsi que la suppression ou la destruction de données personnelles (cf. art. 32, al. 2 LPD). Ces droits ne sont toutefois pas absolus, p. ex. en cas de traitement légal des données (p. ex. dans la domaine du blanchiment d 'argent) ou de traitement des données présentant un intérêt prépondérant pour le responsable du traitement, ces droits ne s 'appliquent pas.	
Chapitre 2	Pas de corrections.	
3.8.1 Dissolution de la banque	Nouvelle réglementation sur les créances privilégiées: Les **comptes de libre passage** et les **comptes du pilier 3a** bénéficient d'une protection supplémentaire, jusqu'à un montant plafond de CHF 100 000.– chacun, l'excédent étant ensuite rattaché à la troisième classe de l'état de collocation. Au total, les créances privilégiées peuvent donc représenter jusqu'à CHF 300 000.– par client.	
Chapitres 4 + 5	Pas de corrections.	

Section	Le blanchiment d'argent
Chapitre 1	Pas de corrections.

<table>
<tr><th>Section</th><th colspan="2">Le blanchiment d’argent</th></tr>
<tr><td>2.2.1 Loi sur le blanchiment d ‘argent (LBA)</td><td colspan="2">La révision de la LBA entraîne un renforcement de l ‘obligation de diligence des intermédiaires financiers à partir du 1.1.2023:

Les obligations de diligence des intermédiaires financiers
La LBA soumet les intermédiaires financiers à six obligations de diligence.
Fig. 2-3 Les six obligations de diligence
 
</td></tr>
<tr><td></td><td>1. Vérification de l’identité du cocontractant</td><td>Pas de relations d’affaires sous un faux nom. La banque doit connaître l’identité de son client (nom, prénom, adresse du domicile, date de naissance et nationalité). Elle doit donc vérifier l’identité de chaque cocontractant. En règle générale, elle exige de ses clients une pièce de légitimation officielle munie d’une photo ou un extrait d’inscription au registre du commerce.</td></tr>
<tr><td></td><td>2. Identification de l’ayant droit économique</td><td>L’ayant droit économique peut être:
Le cocontractant lui-même
Un tiers
Le détenteur du contrôle auprès de personnes morales exerçant une activité opérationnelle ou de sociétés de personnes
La loi sur le blanchiment d’argent vise à favoriser la transparence auprès de personnes morales et physiques, de sociétés de personnes, de trusts, etc.
Pas de relations commerciales avec des «hommes de paille». Il arrive très régulièrement qu’une personne gère des valeurs patrimoniales de tiers ou qu’une entreprise fictive soit créée. Il se peut que ces tiers ayant droit aux fonds déposés demeurent «invisibles».
Pour la banque, cela signifie que le cocontractant est une autre personne que l’ayant droit économique. Afin que ce type de configuration ne puisse être exploitée à des fins de blanchiment d’argent, la banque doit identifier le véritable ayant droit de la fortune / de l’entreprise. Elle ne doit pas autoriser que les fonds d’origine criminelle soient dissimulés derrière la façade d’hommes de paille.
Dans le cas des sociétés de personnes ou des personnes morales exerçant une activité opérationnelle, les hommes de paille doivent être évités et il convient d’identifier les personnes effectivement détentrices du contrôle de l’entreprise. En d’autres termes, la banque doit connaître et identifier le détenteur du contrôle effectif d’une entreprise exerçant une activité opérationnelle non cotée en bourse afin d’éviter que les fonds d’origine criminelle transitent via des entreprises fictives.
L’identification de l’ayant droit économique ne doit pas avoir lieu uniquement en cas de doute, mais dans tous les cas.</td></tr>
<tr><td></td><td>3. Renouvellement périodique de l’identification du cocontractant et de l’ayant droit économique</td><td>Les identifications doivent être répétées périodiquement. La fréquence dépend du risque de la relation d’affaires, mais elle doit être d’au moins tous les 7 à 10 ans. Dans le cas des PEP, la vérification doit avoir lieu chaque année.</td></tr>
</table>

Section	Le blanchiment d'argent	
	4. Obligations de diligence particulière en cas de suspicion ou de risque accru	**Éliminer tous les cas de suspicion.** La banque est tenue de clarifier de manière approfondie l'**arrière-plan** et le **but d'une transaction** ou d'une **relation d'affaires** lorsque: • celles-ci sont inhabituelles ou • que celles-ci comportent un risque accru de blanchiment d'argent ou • que des indices laissent supposer que des valeurs patrimoniales proviennent d'un délit fiscal qualifié, d'un crime au sens du CP ou d'une organisation criminelle. Dans le cas de relations présentant un risque potentiel accru de blanchiment d'argent, les banques sont tenues à des obligations de diligence particulières (voir chapitre 3). Les résultats des clarifications (supplémentaires) doivent être documentés. En fonction de ceux-ci, il doit être décidé si la relation d'affaires doit être • poursuivie, • ou cessée et, • en parallèle si le cas doit être signalé au bureau de communication en matière de blanchiment d'argent. **Exemple:** Un chauffeur de camion reçoit un virement de CHF 100 000.– en provenance d 'Ukraine. Comme un virement d 'un tel ordre de grandeur sort de l 'ordinaire pour un chauffeur de camion, la banque doit procéder à des clarifications supplémentaires. Dans l 'exemple, il s 'avère que le paiement couvre les primes de risque du conducteur pour des trajets dans des zones à haut risque au cours des deux dernières années. Il ne s 'agit donc pas de blanchiment d 'argent.
	5. Obligation d'établir et de conserver des documents	**Garantir l'accessibilité des documents à tout moment.** Les documents concernant le client, les transactions et les démarches de clarification entreprises doivent être conservés afin qu'on puisse y accéder dans le cadre d'une enquête ou d'un contrôle ultérieur.
	6. Mesures organisationnelles	**Adopter une organisation permettant de lutter contre le blanchiment d'argent.** Les intermédiaires financiers prennent dans leur domaine les mesures nécessaires pour empêcher le blanchiment d'argent. Ils doivent notamment veiller à assurer un niveau suffisant de formation du personnel et de contrôle.
Chapitre 2, résumé	Adaptation du résumé en raison du renforcement de l 'obligation de diligence des intermédiaires financiers: Les banques réalisant une activité en Suisse doivent se conformer à six obligations de diligence et à trois obligations en cas de soupçon de blanchiment d'argent. L'autorité de surveillance chargée de faire respecter les dispositions correspondantes est la FINMA. • Les **obligations de diligence** sont: – l'**identification du client,** – l'**identification de l'ayant droit économique** et – le **renouvellement périodique de l'identification du cocontractant et de l'ayant droit économique,** – les **obligations de diligence particulières en cas d'irrégularités,** – l'**obligation d'établir et de conserver des documents** et l'**organisation.**	

Section	Le blanchiment d'argent
Solution exercice 6	Adaptation de la solution de l 'exercice en raison du renforcement de l 'obligation de diligence des intermédiaires financiers: 
3.1.1 Quand effectuer la vérification de l 'identité?	Adaptation des détails en raison du renforcement de l 'obligation de diligence des intermédiaires financiers: **Détails de l'identification lors de l'ouverture d'un compte** L'ouverture d'un compte est l'exemple le plus banal de situation requérant une vérification d'identité. Elle est traitée en détails dans le module «Opérations passives». Voici en bref les points essentiels: • L'identification du client doit avoir lieu **avant l'ouverture du compte.** Un compte (ou un dépôt) est dit ouvert lorsqu'il existe. Si l'identification, notamment celle du détenteur du contrôle et de l'ayant droit économique, est retardée, mais que le nouveau compte présente déjà un avoir, la banque doit s'assurer que les documents manquants seront envoyés sous un délai de 30 jours. Le client n'est pas autorisé à effectuer de retrait pendant cette période. Si la banque ne dispose pas des documents à l'expiration du délai, elle doit bloquer le compte de manière à empêcher aussi d'éventuels dépôts. En cas de soupçon de blanchiment d'argent, la banque ne doit pas rompre la relation d'affaires, mais notifier le problème. Seulement si, dans un délai de 40 jours ouvrables, la banque ne reçoit pas de communication l'identification de déclaration indiquant que des informations communiquées seront transmises à une autorité de poursuite pénale, elle a le droit de mettre fin à la relation d'affaires visée par la communication. En cas de rupture de la relation d'affaires, la banque doit en informer immédiatement l'identification de déclaration. • Pour éviter les fonds anonymes et permettre l'identification des clients, les **livrets d'épargne au porteur** existants doivent être transformés en comptes lors de leur première présentation au guichet. Si le client souhaite clôturer son livret, il doit faire l'objet d'une vérification d'identité, même si le solde est inférieur à CHF 15 000.–. • **Renouvellement de l'identification au cours de la relation d'affaires.** En cas de changement de nom (notamment suite à un changement d'état civil) ou de modification de la raison sociale, les collaborateurs de la banque doivent faire preuve d'autant de diligence que lors de la vérification initiale. L'identification doit être renouvelé périodiquement, chaque année pour les relations d'affaires à risque et à des intervalles de 7 à 10 ans au maximum pour les relations d'affaires peu risquées, conformément aux directives LBA/CDB en vigueur. • Chaque client doit être identifié: les comptes anonymes n'existent pas dans le système bancaire suisse. On compte cependant deux, et seulement deux **exceptions,** qui sont énumérés ci-après. C'est l'unique marge de manœuvre possible: – Dans le cas d'un **compte destiné au dépôt de sûretés pour garantir le paiement d'un loyer** au sens de l'article 257e du Code des obligations, la vérification d'identité n'est pas indispensable. – Les clients qui détiennent exclusivement un compte du pilier 3a ou un compte de libre passage auprès d'une banque ne doivent pas être identifiés.

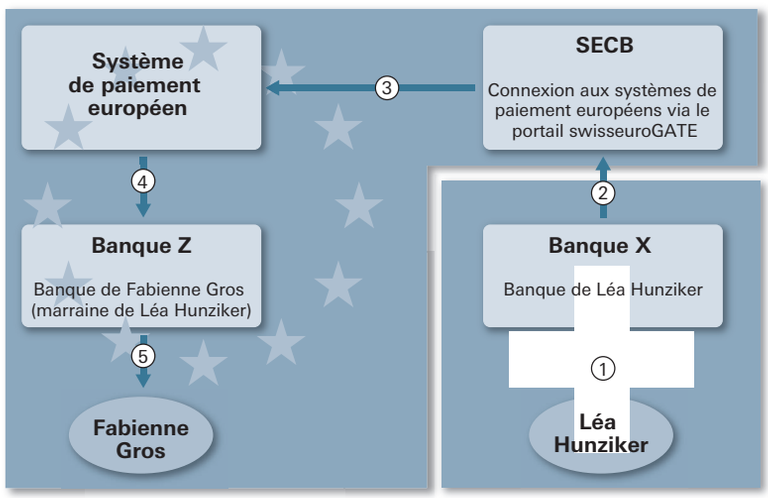
Section	Le blanchiment d'argent
Chapitre 3, résumé	Adaptation du résumé en raison du renforcement de l 'obligation de diligence des intermédiaires financiers: **Identification de l'ayant droit économique** **Le formulaire A** doit être rempli • lorsque la banque sait que le client n'est pas l'ayant droit économique, • lorsque la banque doute que le client soit l'ayant droit économique, • lors de l'établissement d'une relation client par correspondance, • lors d'opérations de caisse d'un montant supérieur à CHF 15 000.–, • dans le cas de sociétés de domicile (exception: sociétés de domicile cotées en bourse) ou • lorsque des avocats ou notaires exercent une activité de gérant de fortune pour le compte de leurs clients.
Chapitre 4	Pas de corrections.

Section	Opérations passives
Chapitres 1 + 2	Pas de corrections.
3.1.1 Respect de la législation en matière de lutte contre le blanchiment d 'argent	Adaptation en raison du renforcement de l 'obligation de diligence des intermédiaires financiers: **Identification du cocontractant et de l'ayant droit économique** La loi sur le blanchiment d'argent confère aux différentes branches impliquées dans l'intermédiation financière le droit à l'autorégulation. Ces branches définissent elles-mêmes des règles de procédure en matière de lutte contre le blanchiment d'argent et les soumettent à l'avis de l'autorité de surveillance. La Convention relative à l'obligation de diligence des banques (CDB) a en effet été établie par les banques avant même la promulgation de la loi sur le blanchiment d'argent. L'une des principales obligations de toute banque est la **vérification de l'identité du cocontractant** (principe du «Know your customer») et de **l'ayant-droit économique** (beneficial owner).

<table>
<tr><th>Section</th><th colspan="2">Opérations passives</th></tr>
<tr><td>3.1.1 Respect de la législation en matière de lutte contre le blanchiment d ’argent</td><td colspan="2">Adaptation des dispositions relatives à la procédure à suivre en cas de soupçon de blanchiment d ’argent et à l ’obligation de conserver les documents d ’identification en raison de la révision de la LBA:
Soupçon de blanchiment d’argent
Que faire lorsqu’un employé de banque qui vérifie l’identité d’une nouvelle cliente soupçonne un cas de blanchiment d’argent?
Dans ce cas, ne pas ouvrir le compte et informer le bureau de communication en matière de blanchiment d’argent, qui initiera la suite de la procédure.
Que faire lorsqu’un employé de banque soupçonne de façon justifiée un client de blanchiment d’argent? La loi sur le blanchiment d’argent définit la procédure suivante:
1. Déclaration immédiate au comité interne de lutte contre le blanchiment d’argent. Toutes les banques doivent être dotées d’un tel comité. L’employé de banque doit faire part de ses soupçons sans délai. Le comité interne prend ensuite le relais.
2. Déclaration immédiate auprès du Bureau de communication en matière de blanchiment d’argent (MROS). En cas de soupçon, le comité interne procède aux clarifications, remplit un formulaire de déclaration et le transfère sans délai au MROS.
3. Clarifications par le Bureau de communication en matière de blanchiment. Pendant ce temps, la banque peut continuer à exécuter les ordres du client.
4. Le Bureau de communication en matière de blanchiment d’argent communique à la banque qu’elle transfère la déclaration à un organisme chargé de l’application de la loi. Les valeurs patrimoniales doivent être bloquées sans délai. Le blocage dure au maximum cinq jours ouvrables. Soit une procédure pénale est ouverte et le blocage est maintenu, soit les valeurs patrimoniales sont débloquées.
5. Si, dans un délai de 40 jours ouvrables, la banque ne reçoit pas de notification indiquant que les informations ont été transmises à une autorité de poursuite pénale, elle a le droit de terminer la relation d ’affaires. Si elle le fait, la banque doit toutefois en informer immédiatement le bureau de communication.
Durant toute la procédure, la personne concernée ne doit pas être informée de la déclaration. Voir également le module «Blanchiment d’argent», section 2.2.1.
Obligation de conservation des documents aux fins de la procédure d’identification
Les banques établissent un dossier pour chaque client. Généralement enregistré électroniquement, ce dossier contient les documents dont la banque a besoin pour contrôler l’identité de ses clients (copie de pièce d’identité, liste de contrôle signée, formulaire A signé, etc.).
Les banques sont tenues de conserver ces dossiers pendant au moins 10 ans, et même jusqu’à la fin de la relation, pour permettre de déterminer le cas échéant si l’identité a été correctement vérifiée. Si l’autorité d’instruction ouvre une enquête sur un éventuel blanchiment d’argent, la banque qui gère le compte concerné doit être en mesure de prouver en détail qu’elle a vérifié l’identité du client avec la diligence requise. Si elle n’est pas en mesure de le faire, elle encourt une peine.</td></tr>
<tr><td>3.3.1 La vérification de l’identité et l ’identification de l ’ayant droit économique lors de l ’ouverture du compte</td><td colspan="2">Adaptation en raison du renforcement de l ’obligation de diligence des intermédiaires financiers:
Si les personnes physiques sont identifiables au moyen d’une pièce d’identité, ce n’est pas le cas des entreprises, qui sont des personnes morales.
Les types d’entreprises précitées sont soumises aux principes suivants lors de la vérification de l’identité et de l’identification de l’ayant-droit économique:
Fig. 3-12 Vérification de l’identité et identification de l’ayant droit économique de personnes morales</td></tr>
<tr><td></td><td>Vérification de l’identité de la personne morale</td><td>• Entreprise sise en Suisse et inscrite au registre du commerce (RC). L’identité est vérifiée à l’aide d’un extrait du registre du commerce qui ne doit pas dater de plus de 12 mois. Étant donné que les offices du registre du commerce peuvent désormais tous être contactés via Internet, le contrôle peut être effectué par voie électronique. La banque a également la possibilité de vérifier si l’entreprise figure sur le registre du commerce via la base de données Teledata ou la feuille officielle suisse du commerce (FOSC).
• Entreprise sise en Suisse et n’étant pas inscrite au RC (associations et autres communautés). L’identité est vérifiée par le biais des statuts (actes de fondation) et du procès-verbal de l’assemblée annuelle. La personne chargée de l’ouverture du compte peut alors prouver que la société existe.</td></tr>
</table>

Section	Opérations passives	
	Vérification de l'identité de la personne physique qui ouvre la relation	L'identité de la **personne physique,** qui ouvre la relation bancaire pour l'entreprise, **doit également être vérifiée** selon la même procédure que pour les cas des particuliers (document d'identité et attestation d'authenticité si l'ouverture de la relation s'effectue par voie de correspondance). Il faut en outre s'assurer que la personne qui ouvre la relation est habilitée à le faire pour le compte de l'entreprise et documenter cette démarche.
	Détermination et identification de l'ayant droit économique	• En plus de la vérification de l'identité, le détenteur du contrôle doit être identifié dans le cas d'**une personne morale ou d'une société de personne non cotée en Bourse exerçant une activité opérationnelle.** En Suisse, les personnes exerçant une activité opérationnelle sont par exemple actives dans les domaines de la production de biens ou de prestations. Le détenteur de contrôle est identifié au moyen d'une déclaration, le **«formulaire K».** • Si le client n'est pas une société exerçant une activité opérationnelle mais une **société de domicile,** l'ayant droit économique des valeurs patrimoniales de la société de domicile doit être identifié au moyen du **«formulaire A».** L 'ayant droit économique doit également être identifié.
Chapitre 3, résumé	Point d 'énumération supplémentaire en cas de soupçon de blanchiment d 'argent: **Soupçon de blanchiment d'argent** En cas de soupçon de blanchiment d'argent, la banque doit procéder comme suit: 1. **Déclaration immédiate** au **comité interne de lutte contre le blanchiment d'argent.** 2. **Déclaration immédiate du comité au Bureau de communication en matière de blanchiment d'argent (MROS).** 3. **Clarifications par le Bureau de communication en matière de blanchiment.** La banque peut continuer à exécuter les ordres du client. 4. Le **Bureau de communication en matière de blanchiment d'argent** décide de la suite de la procédure. En cas de procédure pénale, les **valeurs patrimoniales sont bloquées** pendant **cinq jours ouvrables maximum.** 5. Si, dans un délai de 40 jours ouvrables, la banque ne reçoit pas de notification indiquant que les informations ont été transmises à une autorité de poursuite pénale, elle a le **droit de terminer la relation d 'affaires.** Si elle le fait, la banque doit toutefois en informer immédiatement le bureau de communication.	
	Adaptation en raison du renforcement de l 'obligation de diligence des intermédiaires financiers: **Comptes ouverts par des personnes morales** La procédure d'identification • **Sociétés inscrites au RC:** Extrait du registre du commerce, vérification de l'identité de la personne ouvrant le compte **et** du détenteur du contrôle. • **Sociétés non inscrites au RC:** Statuts/procès-verbal de l'assemblée annuelle, vérification de l'identité de la personne ouvrant le compte **et** du détenteur du contrôle.	
Chapitre 4	Pas de corrections.	

Section	Prestations de base
Chapitre 1	Pas de corrections.
2.2 Traitement des paiements en Europe	Adaptation du point 1 dans la description du graphique:



① Léa Hunziker demande à sa banque (banque X) de virer EUR 300.– sur le compte de sa marraine, Fabienne Gros, détenu à la banque Z. La banque X débite le compte de Gina Hunziker.
② La banque X transmet l'ordre de paiement via euroSIC à la SECB, à Francfort.
③ L'ordre est transmis par la SECB, qui est connectée aux systèmes de paiement européens (notamment à TARGET 2). Le montant de EUR 300.–, qui a été porté au crédit de la banque suisse détenu par la SECB, est porté quelques minutes plus tard au crédit du compte de la banque bénéficiaire (banque Z).
④ La banque Z est informée d'un encaissement. Elle crédite le compte de Fabienne Gros.
⑤ Fabienne Gros est informée du mouvement sur son compte.

Section	La Banque nationale suisse
Tous les chapitres	Pas de corrections.