Bankwesen und Zahlungsverkehr

Updates zur Auflage 2023 – Ausgabe Juni 2024

GENEHMIGT

Swiss Banking

compendio
Bildungsmedien

Die Printausgabe dieses Buchs ist klimaneutral in der Schweiz gedruckt worden. Die Druckerei Edubook AG hat sich einer Klimaprüfung unterzogen, die primär die Vermeidung und Reduzierung des CO_2-Ausstosses verfolgt. Verbleibende Emissionen kompensiert das Unternehmen durch den Erwerb von CO_2-Zertifikaten eines Schweizer Klimaschutzprojekts. Mehr zum Umweltbekenntnis von Compendio Bildungsmedien finden Sie unter: www.compendio.ch/Umwelt

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

Bankwesen und Zahlungsverkehr
Updates zur Auflage 2023 – Ausgabe Juni 2024

Fachlektorat: Fachgremium Lernmedien Swiss Banking
Grafisches Konzept: icona basel gmbh
Realisation, Korrektorat: Compendio Bildungsmedien AG, Zürich
Illustrationen: Valentina Morrone, www.valentinamo.ch
Druck: Edubook AG, Merenschwand

Konzeption: Arbeitsgruppe des CYP unter Leitung von Alexia Böniger, Thomas Hirt, Compendio Bildungsmedien AG und Cyril Locher, Crealogix
Umsetzung: Christoph Gütersloh und Thomas Hirt, Compendio Bildungsmedien AG
Redaktionelle Betreuung der Aktualisierungen: Remy Gerspacher, Compendio Bildungsmedien AG et al.

Artikelnummer: Update
Auflage: 1. Auflage 2024
Ausgabe: 01N24
Sprache: DE
CYP

Korrekturen und Ergänzungen (Juni 2024)

Die Bankenwelt verändert sich laufend. Und so verändert sich auch der Inhalt des Lerntexts von BankingToday (BT) von Jahr zu Jahr. Es ist ein zentrales Anliegen, dass der Inhalt von BT immer aktuell gehalten wird.

Deshalb gibt Compendio Bildungsmedien jedes Jahr eine aktualisierte und korrigierte Fassung von BankingToday heraus.

Dieses Update sorgt dafür, dass auch die Käufer der Auflage 2023 über die jeweils aktuellen Informationen verfügen:

- Dieses Update wird während dreier aufeinanderfolgender Jahre jeweils per Anfang Juni ergänzt und auf www.compendio.ch/bankingtoday publiziert.
- So ist sichergestellt, dass für die Vorbereitung der Abschlussprüfungen im Sommer bzw. im Frühjahr sämtliche Änderungen und Ergänzungen des Lehrmittels bekannt sind.

Tipp: Wir empfehlen, die Änderungen und Ergänzungen des Updates früh in der Vorbereitungsphase im Lehrmittel zu vermerken bzw. in das Lehrmittel zu übertragen. So kann man von einem nicht zu unterschätzenden Repetitionseffekt profitieren.

<table>
<tr><th>Kapitel</th><th>Die Bank 1 – Einführung in die Welt der Banken</th></tr>
<tr><td>Kapitel 1</td><td>Keine Änderungen.</td></tr>
<tr><td>2.1.2 Exkurs: Die Bankengruppen nach der Nationalbankstatistik</td><td>Nach der Übernahme der CS durch die UBS gibt es in der Schweiz nur noch eine einzige Grossbank:
Grossbanken
Die UBS AG ist mittlerweile die einzige Grossbank der Schweiz.

<table><tr><td>Kundenkreis / Geschäftstätigkeit</td><td>Die UBS ist eine Universalbank. Sie zählt in den Bereichen des Private Banking und des Investment Banking zu den grössten Banken der Welt.</td></tr><tr><td>Geografische Tätigkeit</td><td>Trotz der internationalen Ausrichtung ist die UBS auch im Inland sehr aktiv und über Bankgeschäftsstellen in der Schweiz breit vertreten.</td></tr><tr><td>Rechtsform</td><td>Die UBS ist eine Aktiengesellschaft.</td></tr><tr><td>Besonderheiten</td><td>Die Bilanzsumme der Grossbank macht einen bedeutenden Teil der Bilanzsummen aller Schweizer Banken aus. Um die Vertraulichkeit der Daten zu gewährleisten, publiziert die SNB keine detaillierten Zahlen mehr zur Bankengruppe Grossbanken.</td></tr></table></td></tr>
<tr><td>Kapitel 3 + 4</td><td>Keine Änderungen.</td></tr>
</table>

Kapitel	Die Bank 2 – Regulierung, Compliance, Jahresrechnung und Risk Management
1.3.1 Vertiefung zum neuen Datenschutzgesetz (nDSG)	Die Bedeutung des Datenschutzrechts ist in den letzten Jahren ständig gestiegen. Riesige Mengen an Daten stehen heute zur Verfügung, die **erstellt, genutzt, ausgewertet, gespeichert,** aber auch **missbraucht** werden können. Besonders im Bankensektor, wo Personendaten erstellt und weiterverarbeitet werden, ist der Datenschutz in der Regel zusätzlich zum Bankkundengeheimnis zentral, zum Beispiel • bei der Aufnahme neuer Geschäftsbeziehungen mit privaten Kunden (natürliche Personen), • bei der Einstellung neuer Mitarbeiter, • bei Geschäften mit Konkurrenten, bei denen Personendaten z. B. über deren Mitarbeitende bearbeitet werden, oder auch • bei der Erhebung von Personendaten zu Marketingzwecken. **Welches sind die Rechtsgrundlagen?** Das totalrevidierte DSG trat am 1. September 2023 in Kraft und gilt für sämtliche Unternehmen und Branchen, welche die Personendaten von natürlichen Personen bearbeiten, d. h. Personendaten beschaffen, speichern, aufbewahren, verwenden, verändern, bekanntgeben, archivieren, löschen etc. Je nach Geschäftsmodell und Use Case kann es sein, dass die EU DSGVO, zusätzlich zum DSG anwendbar sein kann und zwar auch für Unternehmen mit Sitz in der Schweiz. Der räumliche Anwendungsbereich der EU DSGVO für nicht in der EU niedergelassene Verantwortliche ergibt sich aus Artikel 3 Absatz 2 EU DSGVO. Die Verordnung gilt somit also nicht nur für natürliche Personen mit Wohnsitz in der EU. Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der EU befinden, durch einen nicht in der EU niedergelassenen Verantwortlichen, wenn die Datenverarbeitung im Zusammenhang damit steht, a) betroffenen Personen in der EU oder EWR Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist; b) das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der EU oder EWR erfolgt. Das Datenschutzrecht steht in einem engen Zusammenhang mit dem Bankkundengeheimnis (BankG 47; vgl. dazu Modul «Die Bank 1»), auch wenn sie unterschiedliche Zwecke haben. Das Bankkundengeheimnis erstreckt sich auf natürliche sowie juristische Personen und schützt die Vertraulichkeit des Bankkunden z. B. vor einer Herausgabe der Daten an echte Dritte, während das DSG auf natürliche Personen anwendbar ist und vor allem die informationelle Selbstbestimmung schützen soll. **Ziele des neuen, totalrevidierten Datenschutzgesetzes** Das Datenschutzgesetz bezweckt nicht den Schutz der Personendaten, sondern den Schutz der informationellen Selbstbestimmung derjenigen Person, auf die sich die Personendaten beziehen. Wer Personendaten bearbeitet hat darum sogenannte Bearbeitungsgrundsätze zu beachten und gesetzliche Pflichten zu erfüllen. Die Datenschutzaufsicht unterliegt dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten **(EDÖB).** **Wer kann sich auf das Datenschutzrecht berufen und welche Daten sind betroffen?** Das Datenschutzrecht schützt natürliche Personen, über die Personendaten bearbeitet werden: • **Personendaten** sind alle Angaben (Daten, Informationen), die sich auf natürliche Personen beziehen (z. B. die Telefonnummer, ein Foto eine E-Mail-Adresse, die Sozialversicherungsnummer oder die IP-Adresse). • **Besonders schützenswerte** Personendaten werden vom Gesetzgeber abschliessend bestimmt. Das sind Personendaten über religiöse, weltanschauliche, politische und gewerkschaftliche Ansichten / Tätigkeiten, über die Gesundheit, die Intimsphäre, oder die Zugehörigkeit zu einer Rasse oder Ethnie, genetische oder biometrische Personendaten, die eine natürliche Person eindeutig identifizieren oder über verwaltungs- oder strafrechtliche Verfolgungen oder Sanktionen und Personendaten über Massnahmen der sozialen Hilfe. Ihnen ist bei der Bearbeitung besondere Aufmerksamkeit zu schenken.

Kapitel	Die Bank 2 – Regulierung, Compliance, Jahresrechnung und Risk Management	
	Was ist bei der Bearbeitung von Personendaten zu beachten? Personendaten dürfen nur rechtmässig bearbeitet werden. Das bedeutet, dass nicht gegen Gesetze verstossen und dass die Datenbearbeitung die Persönlichkeit der natürlichen Person nicht widerrechtlich verletzen darf. Bei der Bearbeitung von Daten sind folgende Grundsätze zu beachten: **Abb. 1-7** Grundsätze der Datenbearbeitung (siehe Art. 6 DSG)	
	Rechtmässigkeit und Verhältnismässigkeit und Treu und Glauben	Die Bearbeitung von Personendaten ist **verhältnismässig,** wenn sie sich dazu eignet, den verfolgten Zweck zu erreichen. Dazu müssen die zu bearbeitenden Daten erforderlich sein. In der Regel dürfen mehr Personendaten bearbeitet werden, wenn eine Datenbearbeitung mehrere Zwecke verfolgt. Personendaten werden vernichtet oder anonymisiert, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind – gesetzliche oder private Archivierungspflichten bleiben vorbehalten.
	Zweckbindung und Transparenz	Personendaten dürfen nur zu einem **bestimmten** und für die betroffene Person erkennbaren **Zweck** beschafft werden; sie dürfen nur so bearbeitet werden, dass es mit diesem Zweck vereinbar ist.
	Integrität der Daten (Richtigkeit)	Wer Personendaten bearbeitet, muss sich über deren **Richtigkeit** vergewissern. Dies setzt voraus, dass pro Use Case definiert wurde, welche Anforderungen an die Richtigkeit bestehen. Sie oder er muss alle angemessenen Massnahmen treffen, damit die Daten berichtigt, gelöscht oder vernichtet werden, die im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind.
	Einwilligung	Ist die **Einwilligung** der betroffenen Person ausnahmsweise erforderlich, so ist diese Einwilligung nur gültig, wenn sie für eine oder mehrere bestimmte Bearbeitungen nach angemessener Information freiwillig erteilt wird. Falls eine Einwilligung ausnahmsweise erforderlich wäre, muss sie für folgende Datenbearbeitungen ausdrücklich erfolgen: a) die Bearbeitung von besonders schützenswerten Personendaten; b) ein Profiling mit hohem Risiko durch eine private Person; oder c) ein Profiling durch ein Bundesorgan. d) eine Bekanntgabe in einen ausländischen Staat ohne angemessenes Datenschutzniveau.
	Abb. 1-8 Pflichten bei der Datenbearbeitung	
	Informationspflicht	Wenn Personendaten beschafft werden, muss die betroffene Person darüber **informiert** werden, sofern keine Ausnahmen gemäss Art. 20 DSG greifen. Die betroffene Person muss die Identität, die Kontaktdaten des Verantwortlichen und den Bearbeitungszweck erfahren. Falls die Personendaten an Dritte zur Bearbeitung weitergegeben werden, müssen auch diese bekanntgegeben werden. Werden die Daten nicht bei der betroffenen Person beschafft, so sind der betroffenen Person zudem die Kategorien der bearbeiteten Personendaten mitzuteilen (vgl. Art. 19 Abs. 3 DSG). Werden die Personendaten ins Ausland bekanntgegeben, so sind der betroffenen Person auch der Staat oder das internationale Organ mitzuteilen (vgl. Art. 19 Abs. 4 DSG).

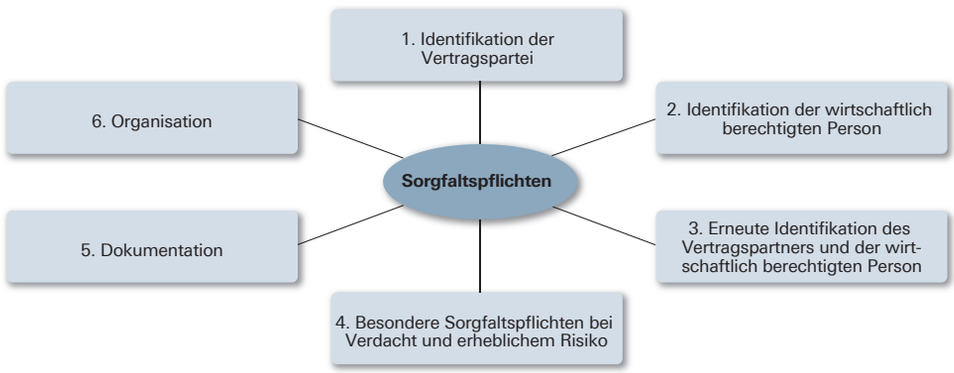
Kapitel	Die Bank 2 – Regulierung, Compliance, Jahresrechnung und Risk Management	
	Verzeichnispflicht	Der Verantwortliche und der Auftragsbearbeiter haben je ein **Verzeichnis ihrer Bearbeitungstätigkeiten** zu führen (vgl. Art. 12 Abs. 1 DSG). **ACHTUNG:** Der Bundesrat sieht Ausnahmen für Unternehmen vor, die weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen und deren Datenbearbeitung ein geringes Risiko von Verletzungen der Persönlichkeit der betroffenen Personen mit sich bringt (vgl. Art. 12 Abs. 5 DSG). • die Identität des Verantwortlichen; • den Bearbeitungszweck; • eine Beschreibung der Kategorien betroffener Personen und der Kategorien bearbeiteter Personendaten; • die Kategorien der Empfängerinnen und Empfänger; • wenn möglich die Aufbewahrungsdauer der Personendaten oder die Kriterien zur Festlegung dieser Dauer; • wenn möglich eine allgemeine Beschreibung der Massnahmen zur Gewährleistung der Datensicherheit; • falls die Daten ins Ausland bekanntgegeben werden, die Angabe des Staates sowie die Garantien.
	Meldepflicht	Kommt es zu einer Verletzung der Datensicherheit («data breach») und führt diese voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person, so muss dies so rasch als möglich **gemeldet** werden. Der Verantwortliche meldet dem **EDÖB** (Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter) so rasch als möglich eine Verletzung der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt. In der Meldung nennt er mindestens die Art der Verletzung der Datensicherheit, deren Folgen und die ergriffenen oder vorgesehenen Massnahmen (vgl. Art. 6 Abs.1 und 2 DSG). Der Auftragsbearbeiter meldet dem Verantwortlichen so rasch als möglich eine Verletzung der Datensicherheit. Der Verantwortliche informiert die betroffene Person, wenn es zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt (vgl. Art. 6 Abs. 3 und 4 DSG).
	Datenschutz-Folgenabschätzung	Aufgrund der rasanten technologischen Entwicklungen sind die Folgen einer Datenbearbeitung nicht immer klar absehbar. Wenn eine Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen mit sich bringen kann, muss deshalb eine **Datenschutz-Folgenabschätzung (DSFA)** erfolgen. Die Datenschutz-Folgenabschätzung enthält eine Beschreibung der geplanten Bearbeitung. Sie muss die Risiken der Datenbearbeitung und die Massnahmen zum Schutz der Persönlichkeit und, sofern anwendbar, der Grundrechte aufzeigen (vgl. Art. 22 Abs. 3 DSG). **ACHTUNG:** Die Datenschutz-Folgenabschätzung muss **vorgängig** erstellt werden.
	«Privacy by design» und «privacy by default»	Der Verantwortliche muss den Datenschutz durch Technik, –sog. **«privacy by design»** –, sowie durch datenschutzfreundliche Voreinstellungen,– sog. **«privacy by default»** –, sicherstellen. Dabei werden rechtliche Vorgaben durch die zuständigen Fachstellen sowie Funktionen in eigenständige Vorgaben für technische und organisatorische Massnahmen (TOM) übersetzt (vgl. Art. 7 DSG).

Kapitel	Die Bank 2 – Regulierung, Compliance, Jahresrechnung und Risk Management	
	Datenweitergabe an Dritte und Übermittlung ins Ausland	Wenn Personendaten weitergegeben oder ins Ausland übermittelt werden, geht die Kontrolle darüber bis zu einem gewissen Grad verloren. Es besteht die Gefahr, dass die Personendaten nicht angemessen geschützt, d. h. vor allem die Bearbeitungsgrundsätze (siehe oben) nicht eingehalten werden können und dadurch die betroffenen Personen in ihren Rechten verletzt werden. Deshalb gelten für die Datenweitergabe und die Übermittlung ins Ausland besondere Regeln. **Datenweitergabe an Dritte:** An sogenannte Auftragsbearbeiter (vgl. Art. 5 lit. k und 9 DSG) dürfen Personendaten weitergegeben werden, wenn dies vertraglich vereinbart wird oder in einem Gesetz vorgesehen und die Datensicherheit gewährleistet ist. **Datenübermittlung ins Ausland:** In Länder, die ein angemessenes Datenschutzniveau gewährleisten, dürfen Personendaten ohne zusätzliche Voraussetzungen bekanntgegeben werden (vgl. Art. 16 DSG). Welche Länder einen «angemessenen» Schutz haben, bestimmt der Bundesrat. Er veröffentlicht eine Liste mit diesen Ländern. Einen angemessenen Schutz bieten z. B. alle Länder der EU.
	Profiling und automatisierte Einzelentscheidungen	**Profiling** ist jede Art der automatisierten Bearbeitung von Personendaten, die darin besteht, dass diese Personendaten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen (Art. 5 lit. f DSG). Beispiel: Automatisierte Erstellung eines Kundenprofils für das Ausspielen massgeschneiderter Online-Werbung oder die Unterbreitung angemessener Anlageempfehlungen. **Automatisierte Einzelentscheidung** ist eine Entscheidung, die ausschliesslich auf einer automatisierten Bearbeitung beruht und die für sie mit einer Rechtsfolge verbunden ist oder sie erheblich beeinträchtigt (Art. 21 DSG). Beispiel: Automatisierte Bonitätsbeurteilungen, um Aufträge eines Kunden im E-Banking automatisiert anzunehmen und auszuführen.
	Welchen Anspruch an seinen Daten hat eine Person? Die von einer Datenbearbeitung betroffenen Personen haben insbesondere folgende Rechte: **Abb. 1-9** Rechte einer von einer Datenbearbeitung betroffenen Person	
	Betroffenenrechte	**Auskunftsrecht:** Betroffene Personen haben in der Regel das Recht, Auskünfte über folgende Informationen zu erhalten (vgl. Art. 26 DSG betreffend Einschränkung, Aufschub und Verweigerung des Auskunftsrechts): • Identität / Kontaktdaten des Verantwortlichen • Bearbeitete Personendaten • Bearbeitungszweck • Aufbewahrungsdauer • Herkunft der bearbeiteten Personendaten • Handelt es sich um eine automatisierte Einzelentscheidung? • Drittempfänger von bearbeiteten Personendaten Der Verantwortliche muss kostenlos, in der Regel innert 30 Tagen, Auskunft erteilen.
	Recht auf Datenportabilität	Jede Person kann vom Verantwortlichen die **Herausgabe ihrer elektronischen Personendaten** verlangen, wenn dieser die Personendaten automatisiert bearbeitet und die Personendaten mit Einwilligung der Person oder in Zusammenhang mit einem Vertrag bearbeitet wurden (vgl. Art. 28 Abs. 1 DSG).
	Recht auf Berichtigung und Recht auf «Vergessenwerden»	Wenn Personendaten unrichtig sind, besteht ein **Recht auf Berichtigung.** Die betroffene Person kann eine solche Berichtigung verlangen, es sei denn, eine gesetzliche Vorschrift verbietet dies oder die Personendaten werden zu Archivzwecken im öffentlichen Interesse bearbeitet. Dasselbe gilt für das **Recht auf Löschung bzw. «Vergessenwerden»:** Ist der Zweck einer Bearbeitung von Personendaten erfüllt und bestehen keine gesetzlichen oder privaten Archivierungsgründe, kann deren Löschung verlangt werden.

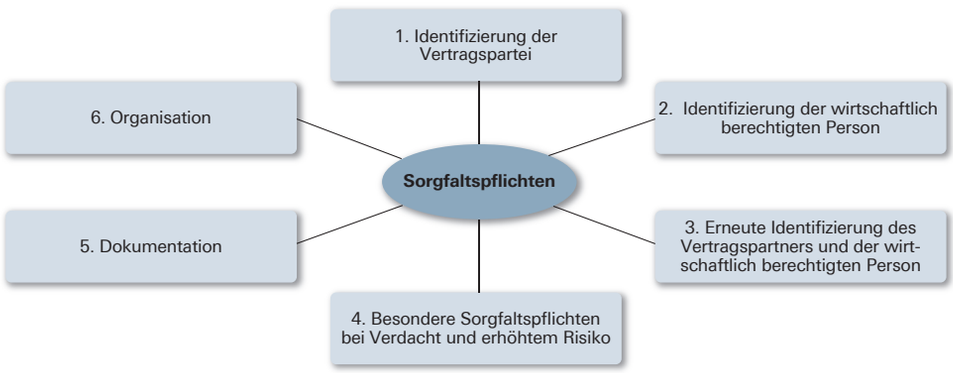
Kapitel	Die Bank 2 – Regulierung, Compliance, Jahresrechnung und Risk Management
	Wann liegt eine Datenschutzverletzung vor? Wenn insbesondere die Bearbeitungsgrundsätze für die Datenbearbeitung nicht eingehalten werden und kein Rechtfertigungsgrund vorliegt, liegt in der Regel eine Datenschutzverletzung, d. h. ein Verstoss gegen das Datenschutzgesetz (DSG) vor. Als **Rechtfertigungsgründe** kommen infrage: • Einwilligung der betroffenen Person • Ermächtigung durch das Gesetz • Überwiegendes privates und / oder öffentliches Interesse
	Beispiel Eine Datenschutzverletzung liegt beispielsweise dann vor, wenn eine Bank öffentlich zugängliche Adressen für Werbezwecke verwendet und die betroffene Person darüber nicht informiert hat (z. B.hat es die Bank versäumt, den betroffenen Personen einen Link zur Datenschutzerklärung in der Werbebroschüre mitzugeben). **Wie kann sich eine Person bei Verstoss gegen das Datenschutzgesetz wehren?** Die betroffene Person kann insbesondere verlangen, dass eine bestimmte Datenbearbeitung verboten wird, eine bestimmte Bekanntgabe von Personendaten an Dritte untersagt wird, Personendaten gelöscht oder vernichtet werden (vgl. Art. 32 Abs. 2 DSG). Diese Rechte gelten jedoch nicht absolut, z. B. bei gesetzlichen Datenbearbeitungen (z. B. im Bereich Geldwäscherei) oder bei Datenbearbeitungen mit einem überwiegenden Interesse der Verantwortlichen greifen diese Rechte nicht.
Kapitel 2	Keine Änderungen.
3.8.1 Auflösung einer Bank	Neue Regelung zu den privilegierten Forderungen: **Freizügigkeitskonti** und **Konti der Säule 3a** sind zusätzlich bis zu einem Betrag von je CHF 100 000.– privilegiert. Alles über dieser Betragsgrenze kommt ebenfalls in die 3. Klasse des Kollokationsplans. Pro Kunde können also max. CHF 300 000.– privilegierte Forderungen sein.
Kapitel 4 + 5	Keine Änderungen.

Kapitel	Geldwäscherei
Kapitel 1	Keine Änderungen.

<table>
<tr><th>Kapitel</th><th colspan="2">Geldwäscherei</th></tr>
<tr><td>2.2.1 Geldwäschereigesetz (GWG)</td><td colspan="2">Durch die Revision des GWG ergibt sich eine verschärfte Sorgfaltspflicht für Finanzintermediäre seit dem 1.1.2023:

Die Sorgfaltspflichten des Finanzintermediärs
Das GwG legt sechs Sorgfaltspflichten für die Finanzintermediäre fest.
Abb. 2-3 Die sechs Sorgfaltspflichten
 
</td></tr>
<tr><td></td><td>1. Identifikation der Vertragspartei</td><td>Keine Geschäftsbeziehungen unter falschem Namen. Die Bank muss wissen, wer ihr Kunde ist.
Deshalb muss sie jeden Vertragspartner mit Name, Vorname, Adresse, Geburtsdatum und Staatsangehörigkeit identifizieren. In der Regel verlangt sie dazu von ihren Kunden einen amtlichen Ausweis mit Foto oder den Auszug des Handelsregistereintrags.</td></tr>
<tr><td></td><td>2. Identifikation der wirtschaftlich berechtigten Person</td><td>Die wirtschaftlich berechtigte Person kann sein:
• Der Vertragspartner selbst
• Eine Drittperson
• Der Kontrollinhaber bei operativ tätigen juristischen Personen oder Personengesellschaften
Das Geldwäschereigesetz möchte die Transparenz bei natürlichen und juristischen Personen, Personengesellschaften, Trusts usw. fördern.
Keine Geschäftsbeziehungen mit «Strohmännern». Immer wieder kommt es vor, dass jemand
Vermögenswerte einer dritten Person verwaltet oder Unternehmen «zum Schein» gegründet werden. Dabei kann es sein, dass diese dritte, am Geld eigentlich berechtigte Person nach aussen gar nicht in Erscheinung tritt.
Für die Bank heisst das Folgendes: Ihre Vertragspartnerin ist eine andere Person als die wirtschaftlich berechtigte. Damit eine solche Konstellation nicht für die Geldwäscherei missbraucht werden kann, muss die Bank wissen, wer die tatsächlich am Vermögen bzw. am Unternehmen berechtigte Person ist und deren Identität überprüfen. Sie darf nicht zulassen, dass sich verbrecherische Gelder hinter der Fassade von «Strohmännern» verstecken können.
Auch bei operativ tätigen juristischen Personen oder Personengesellschaften möchte man Strohmänner vermeiden und die Person(en) identifizieren, die das Unternehmen tatsächlich kontrolliert. Für die Bank bedeutet dies, dass sie die tatsächlich kontrollierende Person(en) eines nicht börsenkotierten, operativ tätigen Unternehmens kennen und identifizieren muss, um zu vermeiden, dass verbrecherischere
Gelder mittels «Scheinunternehmen» abgewickelt werden.
Die Feststellung des wirtschaftlich Berechtigten ist in jedem Fall durchzuführen.</td></tr>
</table>

Kapitel	Geldwäscherei	
	3. Periodische erneute Identifikation der wirtschaftlich berechtigten Person	**Die Identifikationen sind periodisch erneut durchzuführen.** Wie oft hängt vom Risiko der Geschäftsbeziehung ab, jedoch mindestens alle 7 bis 10 Jahre. Bei PEP›s muss die Überprüfung jährlich stattfinden.
	4. Besondere Sorgfaltspflichten bei Verdacht und erheblichem Risiko	**Verdachtsmomente ausräumen.** Die Bank muss die **Hintergründe** und den **Zweck einer Transaktion** oder einer **Geschäftsbeziehung** vertiefter abklären, wenn diese • ungewöhnlich oder • einem höheren Geldwäschereirisiko exponiert sind, oder • bei Anhaltspunkten, dass Vermögenswerte aus einem qualifizierten Steuervergehen, einem Verbrechen nach StGB herrühren oder aus einer kriminellen Organisation stammen. Bei Beziehungen mit einem höheren potenziellen Geldwäschereirisiko haben die Banken besondere Sorgfaltspflichten (siehe Kap. 3, S. 28). Die Ergebnisse der (zusätzlichen) Abklärungen müssen dokumentiert werden. Je nach Ausgang der Abklärungen muss dann entschieden werden, ob die Geschäftsbeziehung • weitergeführt • oder beendigt wird und • parallel dazu entschieden wird, ob an die Meldestelle für Geldwäscherei gemeldet werden muss. **Beispiel:** Ein Lastwagenfahrer erhält eine Überweisung aus der Ukraine über CHF 100 000.–, Da eine Überweisung in solcher Grössenordnung für einen Lastwagenfahrer aus dem gewöhnlichen Rahmen fällt, muss die Bank weitere Abklärungen treffen. Im Beispiel stellt sich heraus, dass die Zahlung die Risikozulagen des Fahrers für Fahrten in Gebiete mit hohem Risiko in den vergangenen zwei Jahren abdeckt. Es geht also nicht um Geldwäscherei.
	5. Dokumentation	**Jederzeitige Auffindbarkeit der Unterlagen.** Die Unterlagen zu einem Kunden, einer Transaktion und zu den getroffenen Abklärungen müssen so aufbewahrt werden, dass sie später bei einer Untersuchung oder zu Kontrollzwecken gefunden werden können.
	6. Organisation	**Organisation, welche die Verhinderung der Geldwäsche sicherstellt.** Finanzintermediäre treffen in ihrem Bereich die Massnahmen, die zur Verhinderung von Geldwäscherei notwendig sind. Sie sorgen namentlich für genügende Ausbildung des Personals und für Kontrollen.
Kapitel 2, Zusammenfassung	Anpassung der Zusammenfassung aufgrund der verschärften Sorgfaltspflicht von Finanzintermediären: **Sorgfalts- und Meldepflichten der Banken** Die in der Schweiz tätigen Banken haben sechs Sorgfaltspflichten und drei Meldepflichten bei Geldwäschereiverdacht. Die FINMA überwacht als Aufsichtsbehörde die Einhaltung dieser Bestimmungen. Die **Sorgfaltspflichten** sind: – die **Identifikation des Kunden,** – die **identifikation des wirtschaftlich Berechtigten** und – die **periodische erneute Identifikation,** – die **besonderen Sorgfaltspflichten bei Auffälligkeiten,** – die **Dokumentation** und – die **Organisation.**	

Kapitel	Geldwäscherei
Lösung Aufgabe 6	Anpassung der Lösung der Aufgabe 6 aufgrund der verschärften Sorgfaltspflicht für Finanzintermediäre: A) 
3.1.1 Wann muss die Identität geprüft werden?	Anpassung der Details aufgrund der verschärften Sorgfaltspflicht für Finanzintermediäre: **Details zur Identifikation bei der Kontoeröffnung** Die Eröffnung eines Kontos ist die alltäglichste Gelegenheit für eine Identifikation. Wir behandeln sie ausführlich im Modul «Passivgeschäft». Hier in aller Kürze das Wichtigste zum Konto: • Die Überprüfung des Kunden muss **vor der Eröffnung** des Kontos stattfinden. Wird die Identifikation Vertragspartners bzw. des wirtschaftlich Berechtigten verzögert, aber weist das neue Konto schon ein Guthaben aus, muss die Bank sicherstellen, dass die fehlenden Unterlagen innert 30 Tagen eingehen. Der Kunde darf in dieser Zeit keine Rückzüge tätigen. Liegen die nötigen Dokumente nach Ablauf der Frist nicht vor, muss die Bank das Konto sperren, sodass auch keine Eingänge mehr gebucht werden können. Besteht Verdacht auf Geldwäscherei, darf die Bank die Geschäftsbeziehung nicht abbrechen und muss Meldung erstatten. Nur wenn die Bank innert 40 Arbeitstagen nach einer erstatteten Meldung keine Mitteilung erhält, dass die gemeldeten Informationen einer Strafverfolgungsbehörde übermittelt werden, darf sie die Geschäftsbeziehung selbst abbrechen. Bei einem Abbruch muss die Meldestelle aber wiederum unverzüglich informiert werden. • Um namenlosen Geldern entgegenzuwirken und die Identifizierung der Kunden zu ermöglichen, sind bestehende **Inhabersparhefte** bei der ersten Vorlage am Schalter in Konti umzuwandeln. Will der Kunde das Sparheft auflösen, muss in jedem Fall eine Identifikation vorgenommen werden – auch bei einem Betrag unter CHF 15 000.–. • **Identifikation während der Geschäftsbeziehung.** Bankmitarbeiter müssen auch bei Namensänderungen (vor allem infolge Zivilstandsänderung) oder Firmenänderungen mit derselben Sorgfalt vorgehen wie bei der ursprünglichen Identifikation. Die Identifikation muss periodisch erneut durchgeführt werden, bei riskanten Geschäftsbeziehungen jährlich, bei wenig riskanten Geschäftsbeziehungen in Abständen von höchstens 7-10 Jahren nach geltenden GwG-/VSB-Richtlinien. • Alle Kunden müssen identifiziert werden. Anonyme Konti gibt es bei den Schweizer Banken nicht. Aber auch hier gibt es **Ausnahmen.** Die nachfolgend aufgezählten Ausnahmen sind die einzigen und es wird kein weiterer Spielraum gewährt: – Bei **Mieterkautionskonti** im Sinne von Art. 257e des Obligationenrechts kann auf eine Identifikationsprüfung verzichtet werden. – Kunden, die ausschliesslich ein Konto der **Säule 3a** oder ein **Freizügigkeitskonto** bei einer Bank führen, müssen nicht durch die Bank identifiziert werden.
Kapitel 3, Zusammenfassung	Anpassung der Zusammenfassung aufgrund der verschärften Sorgfaltspflicht für Finanzintermediäre: **Identifikation des wirtschaftlich Berechtigten** Das **Formular A** muss eingeholt werden, • wenn die Bank weiss, dass der Kunde nicht selbst wirtschaftlich berechtigt ist, • wenn die Bank zweifelt, dass der Kunde selbst wirtschaftlich berechtigt ist, • bei Eröffnung einer Kundenbeziehung auf dem Korrespondenzweg, • bei Kassageschäften über mehr als CHF 15 000.–, • bei Sitzgesellschaften (Ausnahme: börsennotierte Sitzgesellschaften) oder • wenn Anwältinnen oder Notare als Vermögensverwalter auftreten und Gelder ihrer Kunden verwalten.
Kapitel 4	Keine Änderungen.

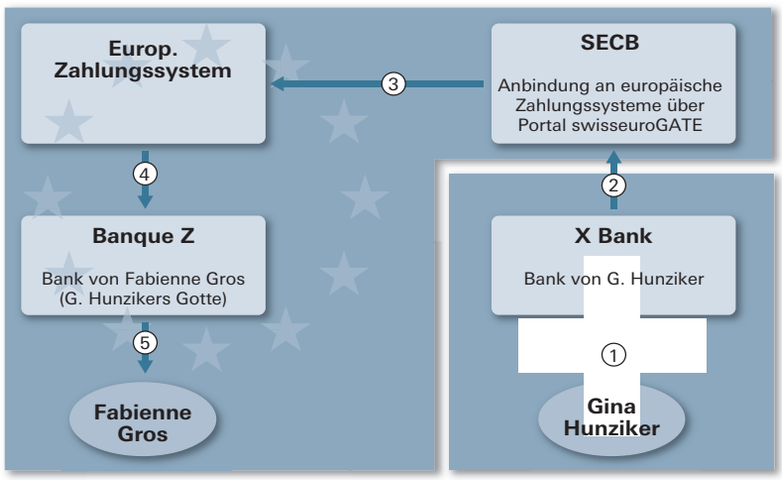
Kapitel	Passivgeschäft
Kapitel 1 + 2	Keine Änderungen
3.1.1 Die Einhaltung der Geldwäschereibestimmungen	Anpassung aufgrund der verschärften Sorgfaltspflicht für Finanzintermediäre: **Den Vertragspartner und den wirtschaftlich Berechtigten identifzieren** Nach dem Geldwäschereigesetz haben die verschiedenen Branchen der Finanzintermediation das Recht zur Selbstregulation. Sie stellen selbst Regeln über das Vorgehen zur Verhinderung von Geldwäscherei auf und sprechen diese mit der Aufsichtsbehörde ab. Mit der Vereinbarung über die Standesregeln zur Sorgfaltspflicht der Banken (VSB) haben die Banken schon vor dem Erlass des Geldwäschereigesetzes solche Regeln aufgestellt. Eine Hauptpflicht der Bank ist, den Vertragspartner und den wirtschaftlich Berechtigten (Beneficial Owner) zu identifizieren.
3.1.1 Die Einhaltung der Geldwäschereibestimmungen	Anpassung der Bestimmungen zum Vorgehen bei Verdacht auf Geldwäscherei sowie zur Aufbewahrungspflicht der Unterlagen zur Identifikation aufgrund der Revision des GWG: **Verdacht auf Geldwäscherei** Was geschieht, wenn eine Bankangestellte bei der Prüfung der Identität einer Neukundin einen Verdacht auf Geldwäscherei entdeckt? In dieser Situation wird das Konto **nicht eröffnet** und der internen Meldestelle für Geldwäscherei gemeldet, welche das weitere Vorgehen initiiert. Was geschieht, wenn ein Bankangestellter bei einem bestehenden Kunden den begründeten Verdacht auf Geldwäscherei hat? Das Geldwäschereigesetz bestimmt folgendes Vorgehen: 1. **Sofortige Meldung an die interne Fachstelle für Geldwäscherei.** Jede Bank muss eine solche Fachstelle haben. Der Bankangestellte muss seinen Verdacht sofort melden. Alles Weitere unternimmt die Fachstelle. 2. **Sofortige Meldung an die staatliche Meldestelle für Geldwäscherei (MROS).** Die Fachstelle für Geldwäscherei trifft Abklärungen, füllt ein Meldeformular aus und leitet dieses im Verdachtsfall sofort an die staatliche Stelle weiter. 3. **Abklärungen durch die Meldestelle für Geldwäscherei.** Während dieser Zeit darf die Bank Kundenaufträge weiter ausführen. 4. **Die Meldestelle für Geldwäscherei teilt der Bank mit, dass sie die Meldung an eine Strafverfolgungsbehörde weiterleitet.** Jetzt müssen die Vermögenswerte unverzüglich gesperrt werden. Diese Sperre dauert maximal fünf Werktage. Entweder wird ein Strafverfahren eröffnet und die Sperre bleibt bestehen oder die Vermögenswerte werden wieder freigegeben. 5. Erhält die Bank innert 40 Arbeitstagen keine Meldung, dass die Informationen an eine Strafverfolgungsbehörde weitergeleitet wurde, hat sie das **Recht, die Geschäftsbeziehung zu beenden.** Wenn sie das tut, muss jedoch die Meldestelle unverzüglich darüber informiert werden. Während des ganzen Ablaufs darf der Betroffene nicht über die Meldung informiert werden. Vergleiche dazu auch das Modul «Geldwäscherei», Kap. 2.2.1. **Aufbewahrungspflicht der Unterlagen zur Identifikationsprüfung** Banken erstellen pro Kunde ein Dossier. Dieses wird oft elektronisch abgespeichert. Im Dossier werden die Unterlagen abgelegt, welche die Bank zur Identitätsprüfung brauchte (z. B. die Passkopie, die unterzeichnete Checkliste, das unterzeichnete Formular A usw.). Die Banken müssen das Dossier mindestens 10 Jahre aufbewahren, damit auch noch nach Jahren und sogar nach Beendigung der Geschäftsbeziehung nachvollzogen werden kann, ob die Identitätsprüfung korrekt war. Eröffnet die Ermittlungsbehörde nämlich eine Untersuchung wegen Geldwäscherei, muss die kontoführende Bank detailliert belegen können, dass sie die Identität des Kunden mit der nötigen Sorgfalt geprüft hat. Kann die Bank diesen Nachweis nicht erbringen, droht ihr deswegen eine Bestrafung.

<table>
<tr><th>Kapitel</th><th colspan="2">Passivgeschäft</th></tr>
<tr><td rowspan="4">3.3.1 Die Identifikationsprüfung und die Feststellung des wirtschaftlich Berechtigten bei der Kontoeröffnung</td><td colspan="2">Anpassung aufgrund der verschärften Sorgfaltspflicht für Finanzintermediäre:

Abb. 3-12 Identifikation und Feststellung des wirtschaftlich Berechtigten bei juristischen Personen</td></tr>
<tr><td>Identifikation der juristischen Person</td><td>• Unternehmen mit Sitz in der Schweiz und Eintrag im Handelsregister (HR). Die Identifikationsprüfung erfolgt mittels Handelsregisterauszug, der nicht älter als 12 Monate ist. Da die Handelsregisterämter inzwischen alle via Internet erreicht werden können, kann die Überprüfung auch auf elektronischem Weg erfolgen. Ebenfalls könnte die Bank mit der Datenbank Teledata oder im Schweizerischen Handelsamtsblatt (SHAB) prüfen, ob das Unternehmen im Handelsregister eingetragen ist.
• Unternehmen mit Sitz in der Schweiz ohne Eintrag im HR (Vereine und andere Gemeinschaften). Hier erfolgt die Identifikationsprüfung über die Statuten (Gründungsakten) und das Protokoll der Jahresversammlung. Damit kann die zur Kontoeröffnung beauftragte Person beweisen, dass die Gesellschaft überhaupt existiert.</td></tr>
<tr><td>Identifikation der eröffnenden natürlichen Person</td><td>Zusätzlich muss auch die natürliche Person identifiziert werden, die die Bankbeziehung für das Unternehmen eröffnet. Das geschieht gleich wie bei Privatpersonen (Ausweis und Echtheitsbestätigung, falls die Eröffnung auf dem Korrespondenzweg erfolgt). Im Weiteren muss abgeklärt und dokumentiert werden, ob der Eröffner überhaupt bevollmächtigt ist, ein Konto für das Unternehmen zu eröffnen.</td></tr>
<tr><td>Feststellung und Identifikation des wirtschaftlich Berechtigten</td><td>• Zusätzlich zur Identifikation muss bei operativ nicht börsenkotierten tätigen juristischen Personen oder Personengesellschaften der Kontrollinhaber festgestellt werden. Operativ tätige juristische Personen sind in der Schweiz z. B. in der Produktion einer Ware oder Dienstleistung tätig. Wer Kontrollinhaber ist, wird mittels Erklärung – des «Formulars K» – festgestellt.
• Ist der Kunde keine operativ tätige Gesellschaft, sondern eine Sitzgesellschaft, muss mittels «Formular A» festgestellt werden, wer wirtschaftlich berechtigt an den Vermögenswerten der Sitzgesellschaft ist. Der Kontrollinhaber/wirtschaftlich Berechtigte muss ebenfalls identifiziert werden.</td></tr>
<tr><td rowspan="2">Kapitel 3, Zusammenfassung</td><td colspan="2">Zusätzlicher Aufzählungspunkt bei Verdacht auf Geldwäscherei:

Verdacht auf Geldwäscherei
Bei Verdacht auf Geldwäscherei muss die Bank wie folgt vorgehen:
1. Sofortige Meldung an die interne Fachstelle für Geldwäscherei.
2. Die Fachstelle nimmt die sofortige Meldung an die staatliche Meldestelle für Geldwäscherei (MROS) vor.
3. Abklärungen durch die Meldestelle für Geldwäscherei. Es dürfen weiter Kundenaufträge ausgeführt werden.
4. Die Meldestelle für Geldwäscherei entscheidet über das weitere Vorgehen. Kommt es zu einem Strafverfahren, werden die Vermögenswerte während maximal fünf Werktagen gesperrt.
5. Erhält die Bank innert 40 Arbeitstagen keine Meldung, dass die Informationen an eine Strafverfolgungsbehörde weitergeleitet wurden, hat sie das Recht, die Geschäftsbeziehung abzubrechen. Wenn sie dies tut, muss sie jedoch die Meldestelle unverzüglich darüber informieren.</td></tr>
<tr><td colspan="2">Anpassung aufgrund der verschärften Sorgfaltspflicht für Finanzintermediäre:

Kontoeröffnung durch juristische Personen
Die Identifikationsprüfung
• Gesellschaften mit HR-Eintrag: Handelsregisterauszug, Identifikation der eröffnenden Person und des Kontrollinhabers.
• Gesellschaften ohne HR-Eintrag: Statuten / Protokoll der Jahresversammlung, Identifikation der eröffnenden Person und des Kontrollinhabers.</td></tr>
<tr><td>Kapitel 4</td><td colspan="2">Keine Änderungen.</td></tr>
</table>

Kapitel	Basisdienstleistungen
Kapitel 1	Keine Änderungen.
2.2 Zahlungsabwicklung in Europa	Anpassung von Punkt 1 in der Beschreibung der Grafik: **Abb 2-6**  ① Gina Hunziker beauftragt ihre Bank X, EUR 300.– dem Konto ihrer Gotte Fabienne Gros bei der Banque Z gutzuschreiben. Die Bank X belastet das Konto von Gina Hunziker. ② Die Bank X leitet die Zahlung von Gina Hunziker via euroSIC an die SECB in Frankfurt weiter. ③ Die SECB ist an die europäischen Zahlungssysteme angeschlossen (vor allem TARGET 2). Sie leitet die Zahlung weiter. Die Zahlung wird auf dem Konto der Schweizer Bank bei der SECB belastet und innerhalb weniger Minuten dem Konto der begünstigten Bank gutgeschrieben. ④ Die begünstigte Banque Z wird über den Eingang einer Buchungsbestätigung informiert. Sie schreibt dem Konto von Fabienne Gros den Betrag gut. ⑤ Sie informiert Fabienne Gros gemäss ihren eigenen Kontobestimmungen über die Gutschrift.
Kapitel 3	Keine Änderungen.

Kapitel	Die Schweizerische Nationalbank
Ganzes Lernheft	Keine Änderungen.