Claudia Keller*/Martin Hess**

Rechtliche Anforderungen an System- und Datensicherheit und Compliance für webbasierte und mobile Zahlungen

Inhaltsverzeichnis

* lic. iur., LL.M., Rechtsanwältin, Wenger & Vieli AG, Zürich.
** Dr. iur., Rechtsanwalt, Wenger & Vieli AG, Zürich.

I. Einleitung

Die Digitalisierung unserer Gesellschaft hat auch schon lange im Banken- und Zahlungswesen Einzug gehalten. Kreditkarten und Zugang zum Bankkonto über das Internet (Online-Banking) gehören mittlerweile zur Standardausstattung und es vergeht kein Tag, an dem nicht ein neues mobiles Zahlungssystem angepriesen wird.[1]

Diese Entwicklung wirft natürlich auch rechtliche Fragestellungen auf, insbesondere in Bezug auf die rechtlichen Anforderungen an die System- und Datensicherheit bei diesen webbasierten und mobilen Zahlungsdiensten. Das Finanzsystem produziert, überträgt, verarbeitet und speichert Unmengen an kundenbezogenen Informationen. Informationssicherheit – verstanden als umfassendes Konzept, das neben der technischen IT-Infrastruktur sämtliche Bereiche abdeckt, die in die Verarbeitung, Übertragung, Speicherung und Sicherung von Informationen involviert sind – ist demzufolge ein zentrales Element des Finanzsystems.[2]

Dies stellt eine grosse Herausforderung für die Compliance-Verantwortlichen der Zahlungsdienstleister dar, denn das Vertrauen ist für die Banken und andere Finanzdienstleister essentiell: Bei einem Leck im Sicherheitsdispositiv und einem Verlust von Kundendaten resultiert nicht nur ein grosser Reputationsverlust, sondern mit den wachsenden regulatorischen Anforderungen können auch ernsthafte rechtliche Konsequenzen daraus entstehen.

Der vorliegende Beitrag soll das Umfeld und die bestehenden rechtlichen Anforderungen insbesondere in Bezug auf die Compliance-Aufgaben für webbasierte und mobile Zahlungen beleuchten.

1 Vgl. das Angebot von Swisscom tapit zur Zahlung per Smartphone. Das Projekt der Six Group steht noch in den Startlöchern. Und auch Apple springt auf den Trend auf und ermöglicht seinen Nutzern mit der neusten Generation von iPhones und einem direkten Deal mit diversen Kreditkartenherausgebern das «Mobile Paying». Weitere Hinweise unter <http://www.20min.ch/finance/news/story/Diese-Bezahl-Apps-haben-die-besten-Erfolgschancen-13620944>. Zum rechtlichen Hintergrund siehe Martin Hess/Alexandra Weiss Voigt, E-Geld, E- und M-Payments gemäss Schweizer Recht, in: CLEARIT März 2014, 8 f.

2 N. Blattner, Referat vom 29. November 2005: IT im Finanzsektor, Aspekte der Regulierung und Überwachung, 2.

II. Ausgangslage

1. Allgemeine Anmerkungen zu Compliance

Compliance ist ein Sammelbegriff für Strategien und Systeme zur Verhinderung von Normverstössen.[3] Als Compliance gilt das Einhalten von gesetzlichen, regulatorischen und internen Vorschriften sowie die Beachtung von marktüblichen Standards und Standesregeln.[4] Gemäss dem 2014 revidierten Swiss Code of Best Practice for Corporate Governance («Swiss Code 2014») umfasst der Begriff Compliance die Einhaltung von Rechtsvorschriften sowie interner Verhaltensrichtlinien (Codes of Conduct, Weisungen). Zur Entwicklung einer unternehmenseigenen Compliance-Kultur ist es notwendig, dass auf allen Ebenen verschiedene Massnahmen getroffen werden, d.h. ein Compliance-Management-System eingeführt wird.[5]

Compliance ist eine andauernde Herausforderung, denn die Unternehmensführung ist gefordert, «die Geschäftstätigkeit und die interne Organisation laufend auf die Einhaltung der verbindlichen Integritätsstandards hin zu überprüfen und erkannte Lücken zeitnah und konsequent zu schliessen».[6]

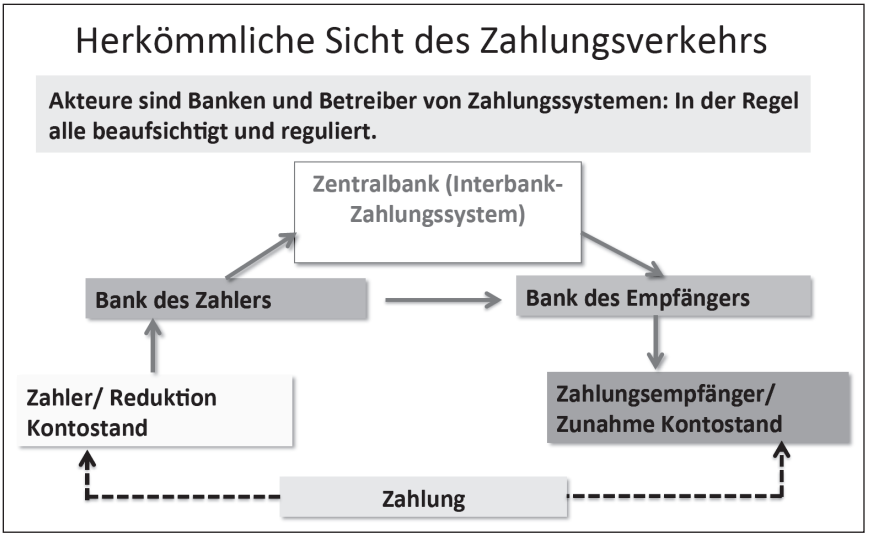
Unabdingbar für jede wirkungsvolle Compliance ist die Kenntnis der rechtlichen Anforderungen in Bezug auf die in Frage stehende unternehmerische Tätigkeit sowie der in diesem Bereich imminenten Risiken. Nachfolgend sollen zunächst die Risiken im Bereich webbasierte und mobile Zahlungen und danach bezogen auf die einzelnen Akteure die rechtlichen Anforderungen in der Schweiz beleuchtet werden.

3 Monika Roth, Compliance in a Nutshell, Zürich St. Gallen 2011, 1.
4 FINMA Rundschreiben 2008/24, Überwachung und interne Kontrolle bei Banken, Rz. 97.
5 David Frick, Der neue Swiss Code of Best Practice for Corporate Governance 2014 in GesKR 4 2014, abrufbar unter <http://www.economiesuisse.ch/de/SiteCollection Documents/Artikel_GesKR_Frick_SwissCode_20150601.pdf>.
6 Gundzüge eines wirksamen Compliance Managements, Hrsg. SwissHoldings und Economiesuisse, September 2014, 2.

2. Risiken im Bereich webbasierte und mobile Zahlungen

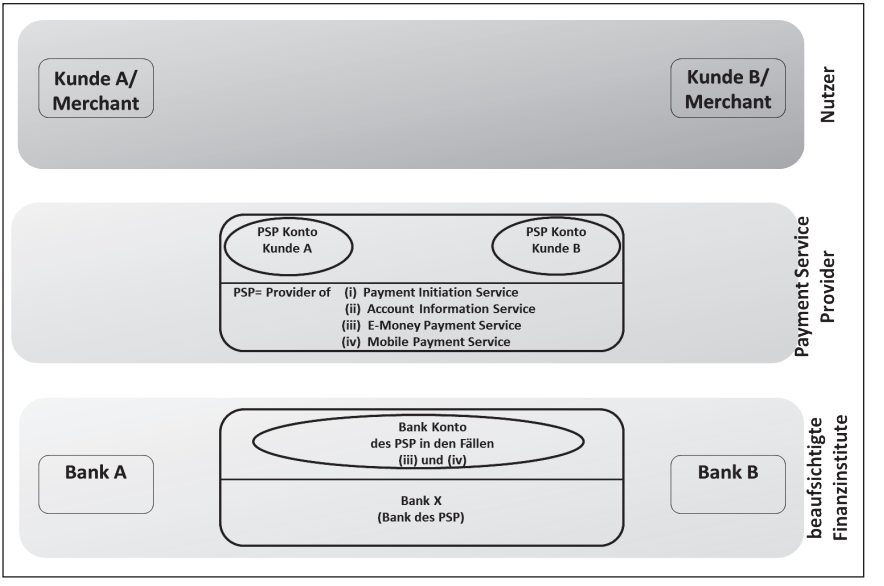
2.1 Vorbemerkungen

Vor 50 Jahren war der Zahlungsverkehr relativ einfach und überschaubar ausgestaltet. Es gab nur wenige Akteure (Banken und Nationalbank oder Post) und eine überschaubare Masse an rechtlichen Anforderungen, primär zu finden im Obligationenrecht und der Gerichtspraxis für das Zivilrecht sowie im Bankgesetz, im Nationalbankgesetz und im Postgesetz für das Aufsichtsrecht.[7]



Heute ist die Welt des Zahlungsverkehrs wesentlich komplexer. Akteure sind nebst den Banken, der Nationalbank und der Postfinance auch Kreditkartenherausgeber, Acquirer, Emittenten von e-money und virtueller Währung und sogenannte Third-Party-Provider (Kontoinformationsdienste [Account Information Services] und Zahlungsauslösedienste [Payment Initiation Services]) insbesondere im mobilen Zahlungsverkehr. Entsprechend komplexer gestaltet sich auch der gesetzliche Rahmen, der zu beachten ist. Es spielen Zivilrecht, Aufsichtsrecht, Strafrecht und Konsumentenschutzrecht zusammen.

7 Vgl. dazu Martin Hess, Euro-Zahlungen gemäss den SEPA-Rulebooks, insbesondere die Haftung der Banken, in: Cross Border Banking, Basel 2009, 47 ff., passim.



Dass webbasierte Zahlungssysteme jeweils häufig auch grenzüberschreitend angeboten werden, macht die Angelegenheit gerade für das Compliance-Management nicht einfacher. Vielmehr ist die Herausforderung, ein möglichst umfassendes Compliance-Management zu implementieren, das den Rahmen des vertretbaren Aufwands nicht sprengt.

Betrachtet man die Risiken im Bereich der webbasierten Zahlungssysteme, scheint dies ein schwieriges Unterfangen.

2.2 Ausgewählte Risiken im Bereich webbasierter Zahlungssysteme

Bei webbasierten oder mobilen Zahlungssystemen gibt es eine Vielzahl von möglichen Risiken; sowohl für die Anbieter der Zahlungssysteme wie auch für die Benutzer. Anbieter von Zahlungssystemen haben Zugriff auf eine Vielzahl von äusserst sensiblen Daten, die gesammelt und zusammengestellt ein umfassendes Bild einer Person zeigen können.[8] Beim Umgang mit diesen Daten ist daher besondere Sorgfalt nötig, um zu verhindern, dass Daten insbesondere weiterverbreitet oder missbraucht werden. Dieses Risiko des Kunden trägt zugleich auch der

8 Heinz Hausheer/Regina E. Aebi-Müller, Das Personenrecht des Schweizerischen Zivilgesetzbuches, Bern 2008, Rz. 13.22.

Anbieter, da er die Daten zu schützen hat. Auch der Beizug Dritter zur Erfüllung von Dienstleistungen, stellvertretend für den Anbieter (Stichworte Intermediatisierung und Outsourcing), kann eine Gefährdung des Datenschutzes darstellen. Gerade die neuen Anbieter im Markt insbesondere im Bereich mobile Payment werben mit der Einfachheit des Zugangs (bspw. über auf das Smartphone herunterzuladende Applikationen) oder durch direkte Integration in Onlineshop-Zahlungsabläufe (Paypal). Diese Anbieter nehmen die Authentisierungsmerkmale der Kunden entgegen und nutzen im Auftrag des Kunden dessen E-Banking Dienste. Die Bank des Kunden ist nicht in der Lage, diese Zugriffe als nicht vom Kunden direkt ausgeführten Zugriff zu identifizieren.

Ein weiteres Risikofeld stellt die Systemverfügbarkeit und -sicherheit dar. Ein Zahlungssystem könnte für längere Zeit nicht verfügbar sein, nur verzögert funktionieren oder gar ganz ausfallen. Das Internet ist ein offenes und weltweit vernetztes Kommunikationssystem. Werden Daten über dieses System transportiert, besteht auch eine grössere Gefahr, dass versucht wird, auf diese Daten zuzugreifen. Es gibt diverse Szenarien, die für den Zugriff auf Daten denkbar sind, wie zum Beispiel Phishing-Attacken, Hackerangriffe in das WLAN-Netzwerk, Installation von schädlicher Software etc.[9] Im Rahmen der Compliance muss daher immer auch ein möglicher Missbrauch durch ein verbotenes Eindringen in das System in das Sicherheitsdispositiv einbezogen werden. Diverse Fälle von Datendiebstahl bei Banken[10] in den letzten Monaten haben gezeigt, dass dies eine grosse Herausforderungen insbesondere für die eingesetzten IT-Systeme darstellt. Die Gefahr von Datendiebstahl kommt aber bei weitem nicht nur von aussen, sondern auch intern gilt es entsprechende Sicherheitshürden zu realisieren, denn die letzten Jahre haben gezeigt, dass auch Mitarbeiter von Zahlungssystem-Anbietern ein entsprechendes Sicherheitsrisiko darstellen können.[11]

Um die modernen Zahlungsmöglichkeiten über E-banking und Smartphones zu ermöglichen, braucht es sodann oft zusätzliche Parteien. Je nach konkreter Gestaltung des angebotenen Zahlungssystems braucht es den Zugang zum Internet, wodurch ein Internet-Service-Provider (ISP) benötigt wird sowie einen Telekommunikations-Service-Provider (TSP). Durch den Einbezug solcher Drittparteien

9 <www.ebankingabersicher.ch/de/ihr-sicherheitsbeitrag/erweiterter-schutz?id=142>.

10 Vgl. bspw. Fälle bei ECB (<http://www.out-law.com/en/articles/2014/july/personal-data-stolen-from-european-central-bank-website-as-ico-issues-separate-data-breach-fine/>) und JP Morgan (<http://www.theguardian.com/money/us-money-blog/2014/oct/03/jp-morgan-data-breach-banks-state-denial>). Zum Rechtlichen siehe Martin Hess, Die Haftung der Banken für Kundendatendiebstahl, in: Bankhaftungsrecht, Basel 2006, 55 ff., passim.

11 Vgl. bspw. Fall Julius Bär (<www.handelszeitung.ch/unternehmen/datenklau-bei-julius-baer-anklage-noch-im-mai>) oder Credit Suisse (<http://www.nzz.ch/aktuell/wirtschaft/wirtschaftsnachrichten/klage-credit-suisse-1.18076845>).

und der «Third-Party-Provider» können sich komplexe Infrastrukturen bilden und es kann zu erhöhten Risiken im Zahlungsverkehr, insbesondere im Bereich der Datensicherheit, kommen.[12] Ein weiteres Risiko stellt der Daten-Zugriff des Third-Party-Providers – Kontoinformationsdienste (Account Information Services) und Zahlungsauslösedienste (Payment Initiation Services) – dar. Dieser hat je nach System und Technologie die Möglichkeit, auf die gesamten Daten zuzugreifen, die im Rahmen seines Angebotes versendet bzw. übertragen werden.[13]

Letztes Glied in der Kette bildet der Kunde selber. Er ist selber gewissen Risiken ausgesetzt, für die er aber häufig selber die Grundlage setzt. Mögliche Risiken für Kunden im Bereich webbasierter und mobiler Zahlungsdienste stellen namentlich die nicht ausreichende Identifizierung und Authentifizierung bei der Registrierung oder beim Auslösen von Zahlungsvorgängen dar. Identitätsdiebstahl und unbewusste Preisgabe von relevanten Kundeninformationen wie PIN-Code und dergleichen durch Manipulation oder Abhören eines Endgerätes stellen genauso ein Risiko dar wie Angriffe bspw. durch Relay-Attacken[14] oder DoS-Attacken[15] häufig ermöglicht durch unsichere Apps, fehlende Schutzmechanismen wie Firewall oder Anti-Viren Software oder veraltete Firmware des Smartphone. Die Zahlungssystem-Anbieter sehen auf der Ebene der Identifizierung und Authentifizieren entsprechende mehrstufige Sicherheitsmassnahmen vor, die der Kunde zu durchlaufen hat, bevor er den Dienst in Anspruch nehmen kann. Solche «Zutrittshürden» bestehen in der Regel aus einer Registrierung kombiniert mit einem oder mehreren Zugangscodes. Aus Gründen der Praktikabilität sind dem Umfang und der Anzahl dieser kundenseitigen Sicherheitsmassnahmen Grenzen gesetzt. Besonders beim Mobile-Payment sind üblicherweise weniger solcher «Hürden» vorhanden, da mit dieser Zahlungsmethode gerade versucht wird, ein möglichst schnelles und bequemes Zahlen zu ermöglichen. Zudem helfen die besten Sicherheitsmassnahmen nicht, wenn der Nutzer des Systems fahrlässig mit seinen Identifikationsmerkmalen oder persönlichen Endgeräten umgeht.

Bevor im nachfolgenden Abschnitt auf die konkreten rechtlichen Anforderungen eingegangen wird, werden kurz die verschiedenen Akteure und allfällige auf diese anwendbare Spezialgesetze skizziert.

12 Vgl. Guidance for a Risk-Based Approach – Prepaid Cards, Mobile Payments and Internet Based Payment Services, FATF, Juni 2013, Art. 53; Mobile Payments: Risk, Security and Assurance Issues, ISACA Emerging Technology White Paper, November 2011, 12.

13 <www.spiegel.de/netzwelt/netzpolitik/britische-regierung-plant-umfassen-des-recht-auf-vorratsdatenspeicherung-a-825 156.html>.

14 Vgl. <http://en.wikipedia.org/wiki/Relay_attack> (in Englisch).

15 Vgl. <http://de.wikipedia.org/wiki/Denial_of_Service> (in Englisch).

III. Rechtliche Anforderungen

1. Akteure im Markt der webbasierten Zahlungssysteme

Auf der einen Seite stehen die regulierten Unternehmen, sprich die Finanzinstitute und die Telekommunikationsanbieter, welche sowohl spezialgesetzlichen wie den für alle Rechtssubjekte geltenden Bestimmungen des Zivilrechts und Regulierungen (z.B. Datenschutzrecht) unterliegen. Auf der anderen Seite – sozusagen als Middle Layer zwischen Finanzdienstleister und Kunden – stehen die nicht spezialgesetzlich regulierten Anbieter von Informatiklösungen (wie bspw. App-Anbieter, Kontoinformationsdienste und Zahlungsauslösedienste). Diese unterliegen den generellen Anforderungen des Datenschutzrechts, Persönlichkeitsrechts sowie der vertragsrechtlichen Sorgfalts- und Treuepflicht. Hinzu kommen gewisse konsumentenschutzrechtliche Bestimmungen wie beispielsweise die Preisbekanntgabeverordnung sowie das Strafrecht.

2. Anforderungen an die Compliance im Bereich webbasierte Zahlungsdienste

2.1 Regulatorische Anforderungen

a Finanzmarktrecht

Ist der Anbieter eines webbasierten oder mobilen Zahlungssystems eine Bank, unterstehen ihre Dienstleistungen den strengen Anforderungen des Bankgesetzes. Ausgangspunkt ist das Bankgeheimnis nach Art. 47 BankG.[16]

Die Anforderungen an die Compliance Funktion und die Risikokontrolle sind in Rz. 100–126 FINMA Rundschreiben 2008/24 *Überwachung und interne Kontrolle bei Banken* umschrieben.[17]

16 Vgl. dazu Hess (Fn. 10), 69 ff.

17 Siehe dazu Othmar Strasser, Interne Untersuchungen, Compliance im Spannungsfeld zwischen Verwaltungsrat, Geschäftsleitung und Mitarbeitenden, in: Banken zwischen Aufsichtsrecht und Strafrecht, Basel 2014, 241 ff., 248 ff. Vgl. auch die «Guidelines on data protection in EU financial services regulation» des European Data Protection Supervisor, abrufbar unter <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Thematic%20Guidelines/14-11-25_Financial_Guidelines_EN.pdf>.

i. FINMA Rundschreiben 2008/21 Operationelle Risiken Banken

Für das Compliance-Management sind insbesondere die von der FINMA im Rundschreiben 2008/21 *Operationelle Risiken Banken* stipulierten Anforderungen von zentraler Bedeutung. Das Rundschreiben wurde Ende 2013 revidiert, um zentrale internationale Standards zum Umgang mit operationellen Risiken in den Schweizer Regulierungsrahmen aufzunehmen. Der Begriff «operationelle Risiken» erfasst hierbei ein weites Spektrum von Ereignissen, die von Rechts- und Betrugsfällen bis hin zu IT-Pannen reichen.[18] Die revidierte Fassung trat am 1. Januar 2015 in Kraft. Im neuen Anhang 3[19] erläutert die FINMA nunmehr in 9 Grundsätze die Anforderungen an ein sachgerechtes Management von Risiken im Zusammenhang mit der Vertraulichkeit elektronischer Personendaten.

Grundsatz 1 Unabhängige Einheit für Compliance

Die Geschäftsführung setzt eine unabhängige Einheit als Kontrollfunktion ein und betraut diese mit der Aufgabe, geeignete Rahmenbedingungen zur Sicherstellung der Vertraulichkeit von Kundendaten zu schaffen und aufrechtzuerhalten. Hierzu soll ein umfassendes Rahmenkonzept geschaffen werden, welches sämtliche Aktivitäten, Prozesse und Systeme/Systemanforderungen in Bezug auf Datenvertraulichkeit berücksichtigt. Die Geschäftsführung ist sodann aufgefordert, die Verantwortlichkeiten und ihre Zuteilung an die verschiedenen Stellen zu definieren und vom Verwaltungsrat genehmigen zu lassen. Die Geschäftsführung hat sodann den Verwaltungsrat regelmässig über die Wirksamkeit der eingeführten Kontrollen zu informieren.

Grundsatz 2 Client Identifiying Data

Dieser Grundsatz befasst sich mit den Kundenidentifikationsdaten (auch «Client Identifying Data» oder abgekürzt «CID»). Die von der Bank verarbeiteten Kundendaten sollen kategorisiert, Kundenidentifikationsdaten festgelegt und in Bezug auf deren Vertraulichkeits- und Schutzstufe kategorisiert werden. In einem nächsten Schritt soll eine Zuordnung der Datenverantwortung erfolgen. Was die Kategorisierung betrifft, so kann zunächst eine Unterscheidung in direkte Kundenidentifikationsdaten, sogenannte DCID, und in indirekte Kundenidentifikationsdaten, sogenannte ICID, gemacht werden. DCID sind alle Daten, die eine direkte Identifikation des Kunden ermöglichen. Darunter fallen Daten wie bspw. Vorname, Nachname, Firmenname, Kontoauszug, E-Mail Adresse, Unterschrift, Profilna-

18 Vgl. Erläuterungen FINMA abrufbar unter <www.finma.ch/d/aktuell/seiten/mm-rs-opr-risiken-banken-20 130 110.aspx>.

19 Erläuterungen dazu abrufbar unter <www.finma.ch/d/regulierung/anhoerungen/Docu-ments/eb-rs-08-21-d.pdf>.

men in sozialen Netzwerken und dergleichen. Diese Daten sind relativ einfach zu kategorisieren. Schwieriger kann es bei den ICID werden. Unter die Kategorie ICID fallen alle Daten, die in Kombination mit einer anderen Information, den Rückschluss auf einen identifizierbaren Kunden ermöglichen. Es handelt sich somit um eine Information, die für sich alleine nicht genügt, einen Kunden zu identifizieren. Welche Informationen darunter fallen, variiert je nach Art und Umfang des Datenverarbeitungssystems und der IT-Infrastruktur bzw. -Architektur. ICID können in drei Unterkategorien unterteilt werden. Als Level 1 ICID werden eindeutig indirekte Identifikationsdaten wie Adresse, Telefonnummern/Faxnummern, Kontonummern/IBAN, Kreditkartennummern und dergleichen qualifiziert. Der Kategorie Level 2 ICID sind Daten zuzuordnen, die möglicherweise eine indirekte Identifikation erlauben. Dazu können Daten wie Geburtsdatum, Familienstand oder IP Adresse gehören. Zur Kategorie Level 3 ICID gehören sogenannte unpersönliche Bezeichner, also Daten wie interne Verarbeitungs-ID oder statisch und dynamisch eindeutige Bezeichner (unique identifiers wie Hardware ID und dergleichen). Level 3 ICID können als Informationen angesehen werden, die nicht CID relevant sind, sofern aus ihnen keine CID abgeleitet werden können und sie niemals im Kundenkontext gezeigt werden.

Grundsatz 3 Datenspeicherort

Transparenz betreffend den Datenspeicherort und -zugriff ist gefordert. Die Bank muss jederzeit wissen, wo CID gespeichert werden, von welchen Anwendungen und Datenverarbeitungssystemen die Daten verarbeitet werden und wer durch welche Mittel elektronisch auf sie zugreifen kann. Angemessene Kontrollen sollen sodann sicherstellen, dass die Daten nach Art. 8 ff. der Verordnung zum Bundesgesetz über den Datenschutz (nachfolgend «VDSG») bearbeitet werden. In Bezug auf allgemeine Massnahmen statuiert Art. 8 VDSG die Pflicht, für die Vertraulichkeit, die Verfügbarkeit und die Integrität der Daten, besorgt zu sein, um einen angemessenen Datenschutz zu gewährleisten *(Datensicherheit)*.[20] Dies beinhaltet insbesondere die Pflicht, die Datenverarbeitungssysteme gegen unbefugte oder zufällige Vernichtung, zufälligen Verlust, technische Fehler, Datenfälschung, Datendiebstahl oder widerrechtliche Datenverwendung sowie gegen unbefugtes Ändern, Kopieren, Zugreifen oder andere unbefugte Bearbeitungen angemessen zu schützen. Die damit zusammenhängenden technischen und organisatorischen Massnahmen müssen insbesondere dem Zweck der Datenbearbeitung, Art und Umfang der Datenbearbeitung sowie der möglichen Risiken für die betroffenen Personen anhand des gegenwärtigen Stands der Technik Rechnung tragen. Einmal festgelegte Massnahmen sind periodisch zu überprüfen und bei Bedarf anzupas-

20 Siehe dazu Hess (Fn. 10), 67 ff., sowie EDÖB, Leitfaden technische und organisatorische Massnahmen, September 2011.

sen. Im Falle einer automatisierten Bearbeitung von Personendaten gelten gemäss Art. 9 VDSG besondere Anforderungen an die technischen und organisatorischen Massnahmen. Diese müssen insbesondere Kontrollen in Bezug auf den Zugang, die Personendatenträger, den Transport, die Bekanntgabe, Speicherung, Benutzung sowie den Zugriff auf und die Eingabe von Daten beinhalten. Entsprechend ist unbefugten Personen der Zugang zu den Einrichtungen, in denen Personendaten bearbeitet werden, zu verwehren. Sodann ist unbefugten Personen das Lesen, Kopieren, Verändern oder Entfernen von Datenträgern zu verunmöglichen. Bei der Bekanntgabe von Personendaten sowie beim Transport von Datenträgern ist zu verhindern, dass die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können. Datenempfänger, denen Personendaten mittels Einrichtungen zur Datenübertragung bekannt gegeben werden, müssen identifiziert werden können. Unbefugte Eingabe in den Speicher sowie unbefugte Einsichtnahme, Veränderung oder Löschung gespeicherter Personendaten sind zu verhindern. Ebenso die Benutzung von automatisierten Datenverarbeitungssystemen mittels Einrichtungen zur Datenübertragung durch unbefugte Personen. Der Zugriff der berechtigten Personen ist auf diejenigen Personendaten zu beschränken, welche die betreffende Person für die Erfüllung ihrer Aufgabe benötigt (Need-to-Know Prinzip). In automatisierten Systemen muss sodann nachträglich überprüft werden können, welche Personendaten zu welcher Zeit und von welcher Person eingegeben wurden. Die automatisierte Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen ist gemäss Art. 10 VDSG zu protokollieren, wenn die präventiven Massnahmen den Datenschutz nicht gewährleisten können.[21] Eine Protokollierung hat insbesondere dann zu erfolgen, wenn sonst nicht nachträglich festgestellt werden kann, ob die Daten für diejenigen Zwecke bearbeitet wurden, für die sie erhoben oder bekannt gegeben wurden. Diese Protokolle sind während eines Jahres revisionsgerecht festzuhalten und dürfen ausschliesslich den Organen oder privaten Personen zugänglich sein, denen die Überwachung der Datenschutzvorschriften obliegt. Sie dürfen auch ausschliesslich für diesen Zweck verwendet werden. Gemäss Grundsatz 3 müssen sodann Bereiche, welche die Speicherung bzw. Zugänglichmachung grosser Datenbestände beinhalten, einer speziellen Kontrolle unterworfen werden.[22]

21 Der Inhaber einer meldepflichtigen automatisierten Datensammlung (vgl. Art. 11a Abs. 3 DSG) hat ein Bearbeitungsreglement zu erstellen, das insbesondere die interne Organisation sowie das Datenbearbeitungs- und Kontrollverfahren umschreibt und die Unterlagen über die Planung, die Realisierung und den Betrieb der Datensammlung und der Informatikmittel enthält. Das Reglement ist regelmässig zu aktualisieren.

22 Dieser Grundsatz gilt nicht für «kleine Banken».

Grundsatz 4[23] *Sicherheitsstandards für die Infrastruktur und die Technologie*

Infrastruktur und Technologie müssen den Schutz von übertragenen und gespeicherten CID am Endpoint (d.h. auf dem Endgerät) gewährleisten. Hierbei ist regelmässig ein Vergleich des internen Rahmenkonzepts zur Sicherstellung der Vertraulichkeit von CID und der Praxis im Markt anzustellen und entsprechende Diskrepanzen auszuwerten und wo nötig entsprechend aufzurüsten.

Grundsatz 5[24] *Anforderungen bezüglich Personal*

Worauf ist bei der Auswahl, Überwachung und Schulung von Mitarbeitenden, die auf CID Zugriff haben, zu achten? Es gilt eine Sorgfaltspflicht bezüglich deren Auswahl sowie eine Schulungs- und Überwachungspflicht. Diese Pflichten gelten auch in Bezug auf Dritte, die im Auftrag der Bank auf Kundenidentifikationsdaten zugreifen können. Für Nutzer und Anwender mit funktionalem Zugriff auf Massen-CID (sog «Schlüsselmitarbeitende») gelten strengere Sicherheitsanforderungen und diese Schlüsselmitarbeitende sind anhand einer Liste zu identifizieren.

Grundsatz 6[25] *Risikoidentifikation und Kontrolle*

Wie sind die Risiken in Bezug auf die CID-Vertraulichkeit zu identifizieren und kontrollieren? Die Identifizierung und Bewertung der inhärenten Risiken und der Restrisiken betreffend die CID-Vertraulichkeit muss mit Hilfe eines strukturierten Prozesses, welcher Risikoszenarien beinhaltet, evaluiert werden. Die zur Sicherstellung des CID-Schutzes definierten Schlüsselkontrollen müssen fortlaufend auf Adäquanz geprüft und bei Bedarf angepasst werden.

Grundsatz 7 Risikominimierung

Dieser Grundsatz setzt sich mit der Aufgabe der Risikominderung in Bezug auf die CID-Vertraulichkeit auseinander und legt fest, dass identifizierte Risiken überwacht und angemessen minimiert werden müssen. Dabei liegt ein spezielles Augenmerk auf Datenbearbeitungen, welche die Veränderung oder Migration grosser CID-Datenbestände betreffen.[26] Stehen strukturelle Veränderungen an, hat sich die Bank rechtzeitig und detailliert mit Sicherheitsmassnahmen in Bezug auf die Vertraulichkeit von CID auseinanderzusetzen.

23 Diese Anforderung gilt nicht für «kleine Banken».
24 Dieser Grundsatz gilt nicht für «kleine Banken».
25 Dieser Grundsatz gilt nicht für «kleine Banken».
26 Nicht anwendbar auf «kleine Banken».

Grundsatz 8 Data Leaks und Kommunikation

Der Grundsatz regelt die Handhabung von Vorfällen im Zusammenhang mit der Vertraulichkeit von CID und die damit verbundene interne und externe Kommunikation. Es wird empfohlen, möglichst rasch auf solche Vorfälle zu reagieren. Damit dies in der Praxis funktioniert, ist sinnvollerweise vorweg eine klare Strategie zur Kommunikation insbesondere bei schwerwiegenden Vorfällen festzulegen und im Ernstfall durchzuziehen. Kontroll- und Prüfergebnisse wie auch Vorfälle sollen überwacht, analysiert und in geeigneter Form dem obersten Management gemeldet werden.

Grundsatz 9 Outsourcing

Der letzte Grundsatz beinhaltet Empfehlungen bezüglich Outsourcing-Dienstleistungen und Grossaufträgen in Verbindung mit CID. Es gilt eine Sorgfaltspflicht in Bezug auf die Auswahl der Anbieter von Outsourcing-Dienstleistungen. Die Bank hat sicherzustellen, dass sie umfassende Kenntnis darüber hat, welche Schlüsselkontrollen der Outsourcing-Dienstleister in Verbindung mit der Vertraulichkeit von CID durchzuführen hat und was seine Aufgabe inhaltlich konkret beinhaltet.

Als besonderes Risiko in Bezug auf die Gewährleistung der Datensicherheit gilt die sogenannte «toxische Kombination». Eine toxische Kombination tritt in Erscheinung, wenn Benutzer aufgrund von fehlerhaften Prozessen, Systemen oder nicht vorhandenen bzw. nicht funktionierenden Zutrittskontrollen auf eine Kombination von sensitiven Daten (bspw. Geburtsdatum plus Adresse) Zugriff haben. Das Risiko entsteht in diesen Fällen durch die Kombination von für sich alleine noch nicht kritischen Daten, deshalb der Begriff «toxische Kombination». Diesem Risiko ist im Rahmen der Massnahmen zur Datensicherheit besonders Rechnung zu tragen. Im FINMA Rundschreiben 2008/7 *Outsourcing Banken* zur Auslagerung von Geschäftsbereichen bei Banken ist in Bezug auf den Datentransfer ins Ausland festgehalten, dass die Kunden mit besonderem Schreiben und detailliert über den Datentransfer zu informieren sind und sie insbesondere auf die getroffenen Sicherheitsvorkehrungen hingewiesen werden müssen, bevor im Rahmen einer Outsourcing-Lösung Daten über Kunden ins Ausland transferiert werden dürfen. Diese besondere Informationspflicht entfällt jedoch, wenn die ins Ausland ausgelagerten Daten keine Rückschlüsse auf die Identität eines Kunden zulassen.[27]

27 Grundsatz 6 des FINMA Rundschreibens 2008/7, *Outsourcing Banken,* RZ 39. Siehe dazu Hess (Fn. 10), 72 ff.

ii. Basel Committee on Banking Supervision: Compliance and the compliance function in banks

Ein älteres, aber nach wie vor wichtiges, Werk in Bezug auf Compliance-Fragen stellt der Leitfaden «Compliance and the compliance function in banks» des Basel Committee on Banking Supervision dar.[28] Die Leitlinien fassen die Pflichten und Aufgaben der verschiedenen Verantwortlichen auf Management- und VR-Ebene in 10 Empfehlungen (in den Leitlinien «Principles» genannt) zusammen.

Compliance-Verantwortliche müssen gestützt auf diese Regelwerke regelmässig folgende Abklärungen treffen:

- Wie sind vorhandene und zukünftige CID zu kategorisieren? Welche Daten sind in welchem Format vorhanden?
- Sind die Systeme zur Datenverwaltung und -verarbeitung geeignet, um aktuelle und anstehende regulatorische Anforderungen zu erfüllen?
- Sind die Daten im Hinblick auf aktuelle und drohende Sicherheitsrisiken angemessen geschützt?
- Sind die Datenverwaltungs- und -verarbeitungssysteme state-of-the-art?

iii. Geldwäschereigesetz

Das Geldwäschereigesetz («GwG») statuiert Sorgfalts- und Kontrollpflichten für Finanzintermediäre, damit das Einschleusen von Vermögenswerten mit verbrecherischem Ursprung in den legalen Wirtschaftskreislauf möglichst weitgehend verhindert wird. Das Betreiben eines Zahlungssystems (bspw. E-Money) ist Finanzintermediation.[29] Die Pflichten der Finanzintermediäre sind in den Art. 3–8 GwG (Sorgfaltspflicht) und Art. 9–11 GwG (Pflichten bei Vorliegen eines Geldwäschereiverdachts) geregelt. Zu den Sorgfaltspflichten der Finanzintermediäre gehören die Identifizierung der Vertragspartei, die Feststellung des wirtschaftlichen Berechtigten, Abklärungspflichten, Dokumentations- und Aufbewahrungspflicht sowie das Treffen geeigneter organisatorischer Massnahmen zu Vermeidung von Geldwäschereitatbeständen. Bei Vorliegen eines Geldwäschereiverdachts treffen den Finanzintermediär eine Meldepflicht, die Pflicht zur Vermögenssperre sowie ein Informationsverbot (zur Verhinderung einer Vorwarnung des Inhabers der betroffenen Vermögenswerte).

28 Abrufbar unter <www.bis.org/publ/bcbs113.pdf>.
29 Art. 2 Abs. 3 Bst. b GwG.

Das GwG ist ein Rahmengesetz, d.h. es statuiert generelle Bestimmungen, welche durch flankierende Verordnungen der FINMA bzw. Regularien der Selbstregulierungsorganisationen konkretisiert werden.[30]

b Datenschutz

Für alle Akteure gleichermassen relevant sind das Datenschutzrecht (Datenschutzgesetz DSG und -verordnung VDSG) und die dazugehörigen Empfehlungen des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten EDÖB.

Die unter dem Datenschutzrecht geschützten Personendaten umfassen alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen (Art. 3 lit. a DSG). Sind Personendaten vollständig anonymisiert, das heisst, sind sie ohne unverhältnismässigen Aufwand nicht einer bestimmten Person zurechenbar, so gelten diese Daten nicht als Personendaten.[31]

Als datenschutzrechtlich relevante Bearbeitung gilt gemäss Art. 3 lit. e DSG jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren. Die Anbieter von webbasierten oder mobilen Zahlungssystemen verwalten und haben Zugriff auf eine Vielzahl von Kundendaten. Darunter beispielsweise Name, Geschlecht, Alter sowie Adresse des Kunden, aber auch Informationen zu seinen getätigten Bezahlungen. Damit bearbeiten sie ohne weiteres Personendaten gemäss DSG.

Gemäss Art. 4 DSG dürfen Personendaten nur rechtmässig beschafft und nur nach Treu und Glauben sowie in verhältnismässiger Weise bearbeitet werden. Die Datenbearbeitung ist zweckgebunden, d.h. die Daten dürfen ausschliesslich zu dem Zweck, der bei der Beschaffung angegeben oder aus den Umständen ersichtlich ist, bearbeitet und verwendet werden.

Das Bearbeiten von Personendaten darf gemäss Art. 12 DSG die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzen, ebenso darf es nicht gegen die Grundsätze in Art. 4 DSG und Art. 6 DSG verstossen. Alle Handlungen entgegen dieser Grundsätze bedürfen eines Rechtfertigungsgrundes gemäss Art. 13 Abs. 1 DSG, namentlich ein überwiegendes privates oder öffentliches Interesse, eine gesetzliche Grundlage oder die Einwilligung des Betroffenen.

Art. 10a DSG regelt sodann die Datenbearbeitung durch Dritte, das sogenannte Outsourcing. Diese Bestimmung ist insbesondere für Anbieter wichtig, die nicht

30 Vgl. Verordnung der Eidgenössischen Finanzmarktaufsicht über die Verhinderung von Geldwäscherei und Terrorismusfinanzierung («GwV-FINMA») vom 8. Dezember 2010.

31 David Rosenthal, Datenschutz im IT-Sourcing, in: Rolf H. Weber/Mathis Berger/Rolf Auf der Mauer (Hrsg.), IT-Sourcing, ICT: Rechtspraxis I, Zürich 2003, 197.

dem BankG und den entsprechenden Vorgaben bezüglich Organisationsstruktur und Outsourcing unterstehen.[32]

Gemäss Art. 10 a Abs. 1 DSG ist die Weitergabe von Daten an Dritte unter den nachfolgenden Vorgaben zulässig:

- Dritte dürfen die Daten nur so bearbeiten, wie es der Auftraggeber selber dürfte (Art. 10a Abs. 1 lit. a DSG);
- der Übertragung darf keine vertragliche oder gesetzliche Geheimhaltungspflicht entgegenstehen (Art. 10a Abs. 1 lit. b DSG); ausserdem
- muss sichergestellt werden, dass der Dritte die Datensicherheit gewährleistet (Art. 10a Abs. 2 DSG).

Dieser Regelung steht bei webbasierten oder mobilen Zahlungssystemen üblicherweise die vertraglich vereinbarte oder gesetzlich geforderte Geheimhaltungspflicht entgegen. Daher bleibt im Falle des Outsourcings nur, die Einwilligung der Kunden einzuholen.

Ein weiteres im Datenschutzrecht verankertes Prinzip ist die *Datensicherheit.* Art. 7 DSG statuiert das Erfordernis, Personendaten durch technische und organisatorische Massnahmen vor unbefugtem Bearbeiten zu schützen. Datensicherheit ist bei jeder Art der Datenbearbeitung i.S.v. Art. 3 lit. e DSG zu gewährleisten.[33] Hierbei beschlagen technische Massnahmen Informationssysteme als solche, während organisatorische Massnahmen das Umfeld des Systems, insbesondere dessen Nutzer, betreffen.[34] Im Vordergrund stehen die Aspekte der Vertraulichkeit, der Verfügbarkeit und der Integrität der Daten.[35] Es muss gewährleistet werden, dass nur berechtigte Personen Zugriff auf die vorhandenen Daten haben, dass die gewünschte Information zum gewünschten Zeitpunkt am gewünschten Ort zur Verfügung steht und, dass die Daten richtig sind und nicht unzulässiger Weise bearbeitet wurden.[36] Eine für die Datensicherheit zentrale Bestimmung ist jene von Art. 8 VDSG. Sie enthält eine nicht abschliessende Aufzählung allgemeiner organisatorischer und technischer Massnahmen, die zu beachten sind, wenn Personendaten bearbeitet oder ein Datenkommunikationsnetz zur Verfügung gestellt wird. Diese Massnahmen müssen insbesondere vor den Risiken der unbefugten oder zufälligen Vernichtung (lit. a), des zufälligen Verlustes (lit. b), des technischen Fehlers (lit. c), der Fälschung, des Diebstahls oder der widerrechtlichen

32 Vgl. vorangehende Ausführungen zum Bankenrecht.

33 BSK-DSG Stamm-Pfister, Basler Kommentar zum Datenschutzgesetz und Öffentlichkeitsgesetz, hrsg. von Maurer-Lambrou/Blechta, Basel 2014 Art. 7 N 3.

34 EDÖB (Fn. 20).

35 BSK-DSG Stamm-Pfister (Fn. 33), Art. 7 N 7.

36 Eva-Maria Belser/Astrid Epiney/Bernhard Waldmann, Datenschutzrecht, Grundlagen und öffentliches Recht, Bern 2011, N 51 zu § 9.

Verwendung (lit. d), des unbefugten Änderns, Kopierens Zugreifens oder der anderen unbefugten Bearbeitung (lit. e) schützen. Art. 8 Abs. 2 VDSG verlangt die Angemessenheit der Massnahmen. Es wird somit keine absolute, sondern immer eine relative, dem Zweck und der Bedeutung der Datenbearbeitung angemessene Sicherheit verlangt.[37] Überdies trägt die Pflicht zur periodischen Überprüfung der Massnahmen nach Art. 8 Abs. 3 VDSG dem stetigen Entwicklungsprozess im Bereich der Datensicherheit Rechnung.[38] Diesen Pflichten unterliegt nicht nur der Dateninhaber, sondern jeder Datenbearbeiter, inklusive der Dritte i.S.v. Art. 10a DSG, der Daten bearbeitet.[39]

Technische Massnahmen, die in Frage kommen sind u.a. die Verwendung von Passwörtern und Firewalls, die das firmeninterne Netz von der Aussenwelt, dem Internet, abschotten. Bei der Datenbearbeitung im Internet sind zudem mehrstufige Schutzvorkehrungen notwendig: Verschlüsselung, Authentisierung, Autorisierung, Prüfspur, sichere Betriebssysteme, digitale Signatur. Gütesiegel und biometrische Systeme erhöhen die Datensicherheit. Überdies braucht es in einem Unternehmen eine aktive Überwachung sowie einen Plan zur Alarmierung, so dass im Falle einer Sicherheitslücke umgehend Gegenmassnahmen ergriffen werden können.[40]

c Fernmelderecht

Für webbasierte oder mobile Zahlungssysteme ist die Verwendung des Internets oder des Telekommunikationsnetzwerkes unumgänglich. Damit kommt es, wie oben beschrieben, regelmässig zum Beizug von Dritten.

Auf solche Internet- und Telekommunikations-Service-Provider ist in der Schweiz das Fernmeldegesetz (FMG) anwendbar. Durch dieses soll unter anderem die Achtung der Persönlichkeitsrechte im Fernmeldeverkehr sichergestellt werden.[41] Erbringer eines Fernmeldedienstes unterliegen einer Meldepflicht gemäss Art. 4 FMG und unterstehen der Aufsicht des Bundesamtes für Kommunikation (BAKOM) gemäss 58 ff. FMG. Aus diesem Erlass ergeben sich überdies gewisse Pflichten im Rahmen der Datenbearbeitung.

Erwerber einer Funkkonzession dürfen gemäss Art. 27 i.V.m. Art. 13a Abs. 1 FMG Personendaten, einschliesslich Persönlichkeitsprofile, bearbeiten, sofern dies zur

37 BSK-DSG Stamm-Pfister (Fn. 33), Art. 7 N 9.
38 BSK-DSG Stamm-Pfister (Fn. 33), Art. 7 N 17.
39 Belser/Epiney/Waldmann (Fn. 36), § 9 N 55, § 10 N 34.
40 Siehe dazu EDÖB, Rede von Odilo Guntern vom 29. Juni 2001, Teil 3 (<www.edsb.ch/d/doku/pressemitteilungen/2001/rede.htm>).
41 Vgl. Art. 1 Abs. 2 lit. b FMG.

Erfüllung der ihnen durch Fernmeldegesetzgebung auferlegten Aufgaben unerlässlich ist. Auch sie müssen jedoch die nötigen technischen und organisatorischen Massnahmen treffen, um den Schutz und die Sicherheit der Daten bei der Bearbeitung, insbesondere bei der Übermittlung, zu gewährleisten (Art. 27 i.V.m. Art. 13a Abs. 2 FMG). Für Standortdaten bestimmt Art. 45b FMG, dass Anbieter von Fernmeldedienste diese nur für gewisse Zwecke bearbeiten dürfen, ansonsten haben sie vorgängig die Einwilligung des Kunden einzuholen oder die Daten zu anonymisieren.[42] Insbesondere beim mobilen Zahlungsvorgang werden standortspezifische Daten beim Point of Sale gespeichert, weshalb diese Bestimmung schutzrechtlich von Relevanz ist.

Überdies unterstehen die Erbringer von fernmeldedienstlichen Aufgaben einer Geheimhaltungspflicht i.S.v. Art. 43 FMG bezüglich Informationen über den Fernmeldeverkehr von Teilnehmern. Die Bestimmungen des Datenschutzrechts sind subsidiär ebenfalls anwendbar (vgl Art. 89 der Verordnung über Fernmeldedienste FDV).

In Bezug auf die Dienstesicherheit regelt Art. 87 FDV, dass Fernmeldedienstanbieter ihre Kunden über die Abhör- und Eingriffsrisiken informieren müssen, welche die Benützung ihrer Dienste mit sich bringt. Ausserdem müssen sie ihnen geeignete Hilfsmittel zur Beseitigung dieser Risiken anbieten oder nennen. In den Richtlinien des BAKOM zur Sicherheit und Verfügbarkeit von Fernmeldeinfrastrukturen und -diensten (BAKOM, Mai 2009) sind entsprechende Compliance-Massnahmen aufgeführt. So müssen Fernmeldedienstanbieter gemäss dieser Richtlinie ein Information Security Management System (ISMS) ausarbeiten und implementieren. Ausserdem stipuliert die Richtlinie, dass nach dem Modell: Plan – Do – Check – Act (in regelmässigem Durchlauf) vorgegangen werden muss, unter Anwendung anerkannter Normen im Bereich Sicherheit von Informationen und Fernmeldeinfrastrukturen.

Sodann haben die Anbieter von Fernmeldediensten zudem auch nach dem Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) gewisse Pflichten zu erfüllen. So sind sie gemäss Art. 15 Abs. 1 BÜPF d. verpflichtet, den gesamten Fernmeldeverkehr, die Teilnehmeridentifikation sowie Verkehrs- und Rechnungsdaten bereitzustellen. Insbesondere sind diese Informationen nach Abs. 2 dieses Artikels 6 Monate zu speichern. Die Informationen unterstehen dabei dem Post- und Fernmeldegeheimnis nach Art. 321ter StGB.[43]

42 Sind Personendaten vollständig anonymisiert, so gelten diese Daten nicht als Personendaten, siehe Rosenthal (Fn. 31), 197.

43 Vgl. Art. 15 Abs. 7 BÜPF.

2.2 Vertragsrechtliche Anforderungen

Bei der Benutzung von webbasierten oder mobilen Zahlungssystemen liegt üblicherweise ein Auftragsverhältnis zwischen dem Anbieter des Dienstes und dem Benutzer vor. Der Beauftragte bzw. der Anbieter des Zahlungssystems ist zur getreuen Geschäftsführung nach Art. 398 OR verpflichtet und untersteht somit der auftragsrechtlichen Sorgfalts- und Treuepflicht. Vom Beauftragten wird gefordert, alles zu tun, um die richtige Erfüllung der Hauptleistung und die Verwirklichung des Leistungserfolges zu sichern und dabei das Integritätsinteresse des Gläubigers zu beachten. Unsachgemässes, unsorgfältiges Verhalten wird deshalb grundsätzlich als Vertragsverletzung aufgefasst.[44]

Wie vorangehend erläutert, gibt es beim mobilen und webbasierten Zahlungsverkehr zahlreiche Faktoren, welche die richtige Erfüllung sowie den Schutz des Kunden gefährden können. Der Benutzer eines mobilen oder webbasierten Zahlungssystems muss ein hohes Vertrauen in den Anbieter haben, da er diesem viele private, personenbezogene Daten überliefert.[45] Diesem Vertrauen muss der Beauftragte mit genügender Sorgfalt beim Umgang mit diesen Daten entgegenkommen.

Bezüglich des mobilen und webbasierten Zahlungsverkehrs stehen die Aufklärungspflichten bezüglich möglicher Risiken sowie Benachrichtigungspflichten bei Eintritt von Systemfehlern oder Gefährdungen der Datensicherheit des Kunden im Vordergrund. Banken sind im Rahmen ihrer Sorgfaltspflicht verpflichtet sicherzustellen, dass sensitive Daten wie bspw. CID geschützt sind. In den AGB werden Kunden entsprechend verpflichtet, ihre Authentisierungsmerkmale für die Nutzung der von E-Banking nicht an Dritte weiterzugeben. Wie eingangs erläutert, geschieht bei der Inanspruchnahme von Diensten Dritter (Apps, Digital Wallets, etc.) aber genau dies. Ohne die Weitergabe der Kundendaten könnte der Kunde diese Drittdienste gar nicht in Anspruch nehmen. In vielen AGB finden sich zudem Haftungsbeschränkungen oder gar -ausschlüsse[46]. Durch solche Haftungsausschlüsse besteht für den Kunden primär die Gefahr, einen grossen Teil möglicher Haftungsrisiken selber tragen zu müssen, selbst wenn er dafür nicht verantwortlich ist. Für den Verfasser der AGB hingegen kann es dazu kommen, dass seine AGB einer gerichtlichen Kontrolle nicht standhalten und er somit die Haftungsrisiken nicht wirksam auf seinen Kunden überwälzen konnte (Art. 8 UWG).

---

44 Walter Fellmann, Berner Kommentar, Bd. IV/2/2, Der einfache Auftrag, Art. 394–406 OR, Bern 1992, N 21 zu Art. 398 OR.

45 Beim mobilen Zahlungsverkehr umfassen diese insbesondere auch geographische Standortdaten, welche als Personendaten im Sinne des DSG qualifiziert werden. Vgl. dazu Gasser Urs, Rechtliche Aspekte des M-Commerce, in: SZW 2002, 13 (19 f.).

46 Beispiele siehe Hess (Fn. 10), 70 ff.

Neben ungenügenden AGB besteht auch die Gefahr ungenügender Einwilligungen. Holt der Anbieter eines Zahlungssystems eine Einwilligung ein, um die Daten des Kunden rechtmässig bearbeiten zu dürfen, muss die Einwilligung gewisse Voraussetzungen erfüllen. Besonders bei Einwilligungen über AGB, General- oder Blankovollmachten ist Vorsicht geboten, da dort oft der wirkliche Umfang der Bearbeitung nicht komplett dargelegt wird.[47] Die Einwilligung kann dadurch unwirksam sein und so zu einer widerrechtlichen Datenbearbeitung durch den Anbieter führen.

IV. Sanktionen: Überprüfung der Einhaltung der Regeln

1. FINMA

Die FINMA hat verschiedenste Massnahmen gegen Verletzungen der gesetzlichen Vorgaben durch Finanzinstitute zur Verfügung. Sie kann die fehlbare Partei rügen (Feststellungsverfügung, Art. 32 FINMAG), spezifische Anordnungen zur Wiederherstellung des ordnungsgemässen Zustands erlassen (Art. 31 FINMAG), gegen natürliche Personen ein Berufsverbot (Art. 33 FINMAG) oder ein Tätigkeitsverbot als Händler verhängen (Art. 35a BEHG). Sie kann auch einen Bewilligungsentzug (Art. 37 FINMAG) aussprechen. Je nach betroffener Partei führt ein solcher Bewilligungsentzug zur Liquidation (z.B. Art. 23^{quinquies} BankG) und bei Überschuldung zur Konkurseröffnung (z.B. Art. 37 FINMAG i.Vm. Art. 25ff. BankG). Die FINMA kann sodann die Einziehung unrechtmässig erzielter Gewinne oder vermiedener Verluste (Art. 35 FINMAG) anordnen. Ebenfalls möglich ist die Veröffentlichung einer rechtskräftigen aufsichtsrechtlichen Verfügung (Art. 34 FINMAG). Bei Dringlichkeit kann die FINMA auch vorsorgliche Massnahmen (Art. 31 FINMAG, Art. 25ff. BankG) erlassen.

Bei einer Verletzung einer Meldepflicht nach GwG kann der fehlbare Finanzintermediär gebüsst werden (bei Vorsatz bis zu CHF 500 000, bei Fahrlässigkeit CHF bis zu 150 000, im Wiederholungsfall mindestens CHF 100 000). Adressaten einer Busse sind bei juristischen Personen grundsätzlich deren Organe, welche die organisatorischen Massnahmen zur Verhinderung der Geldwäscherei und Terrorismusfinanzierung zu treffen haben (vgl. Art. 8 GwG).

47 BSK-DSG Maurer-Lambrou/Steiner (Fn. 33), Art. 4 N 16i.

2. BAKOM

Die Aufsicht gemäss Art. 58 FMG obliegt dem BAKOM. Stellt dieses eine Rechtsverletzung fest, so kann es von der für die Verletzung verantwortlichen juristischen oder natürlichen Person verlangen, den Mangel zu beheben oder Massnahmen zu treffen, damit die Verletzung sich nicht wiederholt. Dem BAKOM ist Auskunft über die getroffenen Massnahmen zu erteilen. Das BAKOM kann sodann den Einzug von Einnahmen anordnen. Bei konzessionierten Betrieben kann das BAKOM die Konzession durch Auflagen ergänzen oder sie einschränken, suspendieren, widerrufen oder entziehen. Es kann auch die Tätigkeit der für die Verletzung verantwortlichen juristischen oder natürlichen Person einschränken, suspendieren oder ganz verbieten.

3. EDÖB

Der EDÖB hat gemäss Art. 27 DSG nur die Aufsicht über die Bundesorgane. Nach Art. 29 DSG kann er im Privatrechtsbereich nur in gewissen Fällen Abklärungen treffen sowie nur Empfehlungen aussprechen.[48] Wird eine solche Empfehlung nicht befolgt oder abgelehnt, kann der EDÖB die Angelegenheit dem Bundesverwaltungsgericht zum Entscheid vorlegen.

Die Verletzung der Auskunfts-, Melde- und Mitwirkungspflichten sowie die Verletzung der beruflichen Schweigepflicht durch Privatpersonen werden auf Antrag der geschädigten Person(en) gemäss Art. 34 bzw. 35 DSG mit Busse bestraft.

V. Ausblick

Es ist damit zu rechnen, dass die Angebote im Bereich der webbasierten Zahlungsdienste weiter zunehmen werden. Die Banken machen den Zugang zum

48 2014 wurde eine parlamentarische Initiative eingereicht (Nr. 14.404), welche verlangt, dass der EDÖB ermächtigt wird, bei einer Verletzung von Bestimmungen des Bundesrechts über den Datenschutz wirksame, verhältnismässige und abschreckende Verwaltungssanktionen in Form von Verwaltungsbussen auszusprechen. Die Höhe der Verwaltungsbusse soll unter Berücksichtigung der Art, der Schwere und der Dauer der Verletzung und abhängig davon, ob eine Widerhandlung vorsätzlich oder fahrlässig begangen wurde, festgelegt werden. Bei Ausübung der Verletzung durch eine juristische Person mit gewinnorientierter Tätigkeit soll die Busse in besonders schwerwiegenden Fällen bis zu 10 Prozent des Umsatzes betragen können. Die Initiative wurde in den Räten bis dato noch nicht behandelt.

Bankkonto auf schriftlichem Wege zusehends unattraktiv und forcieren elektronischen Zugangsverfahren zu Bankeinlagen wie Debit- oder Kreditkartenzahlung oder über Mobile Phones/Laptop. Dies und die Klick-and-Shop Mentalität vieler Kunden wird wohl dazu führen, dass Mobile Payment stark an Bedeutung gewinnen wird.

Wie die obigen Ausführungen gezeigt haben, sind nur die Finanzinstitute der strengen Finanzmarktregulierung unterstellt. Andere Akteure im Bereich webbasierter Zahlungssysteme (Aquirer, Third-Party-Provider) unterstehen nur den allgemeinen Bestimmungen des Datenschutzgesetzes und vertraglich begründeten Treue- und Sorgfaltspflichten.

Im Ausland gibt es Reglungen für e-money Anbieter, Zahlungsdienstleister etc. In der Schweiz besteht hinsichtlich der anwendbaren Regeln für Anbieter webbasierter und mobiler Zahlungsdienste Rechtsunsicherheit. Die rechtliche Qualifizierung neuer Zahlungssysteme wie Mobile Payment sollte klar sein. Das ist gegenwärtig nicht der Fall. E-Geld gilt in der EU nicht als Publikumseinlage.[49] In der Schweiz gilt E-Geld als Publikumseinlage, was zur Anwendung des Bankengesetz führt, ausgenommen die Ausnahmen gemäss Art. 5 Bankverordnung und Rz. 18[bis] FINMA Rundschreiben 2008/3 *Publikumseinlagen bei Nichtbanken* – (i) nur für Waren und Dienstleistungen, (ii) kein Zins, (iii) maximales Guthaben CHF 3000) – sind erfüllt. Damit hinkt die Schweiz hinter dem Ausland hinterher, welches spezifische Normen für Zahlungsdienstleister und Herausgabe von elektronischem Geld kennt.[50] Es bestehen nicht gleich lange Spiesse für Schweizer Anbieter und ausländische Anbieter, die aus dem Ausland für Schweizer Nutzer tätig sind. Ausländische E-Geld Anbieter und Zahlungssystem können ohne physische Präsenz in der Schweiz aus dem Ausland umfassendere Dienstleistungen anbieten können, als dies die geltende Rechtslage in der Schweiz erlaubt.

Hier ist Regulierung angezeigt, um Rechtssicherheit zu schaffen. Als Grundlage der Regulierung bieten sich Art. 81 f. des Entwurfes für ein Finanzmarktinfrastrukturgesetz (E-FinfraG[51]) an. Art. 82 E-FinfraG erlaubt dem Bundesrat, Regelungen für Zahlungssysteme festzulegen, namentlich falls dies zur Umsetzung anerkannter internationaler Standards notwendig ist.

49 Art. 6 Abs. 2 Richtlinie 2009/110/EG vom 16. September 2009 über die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten bestimmt «E-Geld-Instituten ist die Entgegennahme von Einlagen oder anderen rückzahlbaren Geldern des Publikums gemäß Artikel 5 der Richtlinie 2006/48/EG untersagt.»

50 Siehe in der EU die Richtlinie 2007/64/EG vom 13. November 2007 über Zahlungsdienste im Binnenmarkt (vgl. dazu Hess (Fn. 7), 55 ff.) sowie die E-Geldrichtlinie (Fn. 49).

51 Botschaft zum Finanzmarktinfrastrukturgesetz vom 3. September 2014, BBl. 2014, 7483 ff.

VI. Anhang: Compliance relevante Dokumente

1. Auflistung

- **Basel Committee on Banking Supervision, Compliance and the compliance function in Banks, April 2005,**
  <http://www.bis.org/publ/bcbs113.pdf>
  Soft Law
- **FATF, Guidance for a risk-based approach, Prepaid Cards, Mobile Payments and Internet-based Payment Services, June 2013**
  <http://www.fatf-gafi.org/media/fatf/documents/recommendations/guidance-rba-npps.pdf>
  (verbindliches) Soft Law
- **FINMA-Rundschreiben 2008/21: Operationelle Risiken Banken, Anhang 3**
  <http://www.finma.ch/d/regulierung/Documents/finma-rs-2008-21.pdf>
  Verbindlich für regulierte Finanzinstitute
- **Data Leakage Protection**
  Information on Best Practice by the Working Group Information Security of the Swiss Bankers Association
  Selbstregulierung
- **EDÖB,** Dokumente unter **Internet und Computer** und **Leitfäden**
  <http://www.edoeb.admin.ch/datenschutz/00683/index.html?lang=de>
  <http://www.edoeb.admin.ch/datenschutz/00628/00629/index.html?lang=de>
  Know How und Best Practice
- **ECB-Recommendations for the security of internet payments**
  Final version after public consultation
  <https://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf>
  Empfehlungen, Implementierung fand am 1. Februar 2015 statt
- **ECB-Final Recommendations for the security of payment account access services**
  <https://www.ecb.europa.eu/pub/pdf/other/pubconsultationoutcome201405securitypaymentaccountaccessservicesen.pdf>
  «Minimum Expectations»: Verbindliches Soft Law

- **Vorschlag für eine EU-Richtlinie über Massnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union**
  <http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_de.pdf>
  Finaler Vorschlag, Vorwirkungen
- **Richtlinien zur Sicherheit und Verfügbarkeit von Fernmeldeinfrastrukturen und –diensten (BAKOM, Mai 2009)**
  Minimum Standard für Gesetzeskonformität

2. Zusammenfassung Kernpunkte wirksamer Compliance

Security Policy

- Definition eines Rahmenkonzeptes von Aktivitäten und Prozessen betreffend Datensicherheit und Datenvertraulichkeit;
- Dauernde Anpassung an neue Entwicklungen;
- Abhängig von Grösse und Komplexität des jeweiligen Providers.

Risiko Assessment

- Externe Risiken;
- Operationelle Risiken.

Risikokontrolle und Risikominderung

- Dataminimisation (nur die Daten bearbeiten, die es wirklich braucht);
- Need to know (nur Personen involvieren, die wirklich notwendig sind);
- Auswahl der Systeme und der Mitarbeiter.

Kontrollen (Monitoring)

- Fraud Detection Systems und Möglichkeit zur Blockierung;
- Traceability (Nachverfolgung der Transaktion muss möglich sein).

Schutz sensitiver Daten

- Verschlüsselung;
- Trennung zwischen Zugriffsdaten (Customer Authentication) und Autorisierung;
- Trennung zwischen Zugriffsdaten und Transaktionsdaten (IBAN Empfänger, Referenznummer, Überweisungsbetrag);

- Trennung der Kommunikationswege pro Serviceprovider – keine Vermischung der Kommunikationswege bei einem Serviceprovider.

Einführung von Limiten

- Hinsichtlich der Höhe der einzelnen Transaktionen;
- Hinsichtlich des jährlichen Maximalumsatzes;
- Hinsichtlich geografischer Anwendung (Sperren einzelner Länder).

Disaster Recovery Vorsorge

- Backup-Systeme;
- Geheimnisschutz und Rechtliche Massnahmen (siehe US inquiries).

Kundeninformation und Bewusstmachung

- Hinweis auf die Notwendigkeit des Passwortschutzes und der vertraulichen Behandlung der Zugangsdaten;
- Der Notwendigkeit der dauernden Updates für die verwendeten Geräte (Laptops, Tablets, Mobile Phones);
- Sicherheit des Netzwerks und der Netzwerkumgebung.