Kooperationsformen zwischen Banken und Drittanbietern aus vertrags- und datenschutzrechtlicher Perspektive

Cornelia Stengel | Elena Rüegg | Jessica Kim Sommer | Luca Stäuble | Benedikt Freund*

Open Banking or Open Finance essentially means the exchange of financial data between different financial service providers including third party providers at the request of the customer. From a civil liability and data protection perspective this paper examines the legal relationships between banks, third party providers, platforms and customers on the basis of four possible «model forms of cooperation»: (1) outsourcing, (2) joint offers by banks and third party providers, (3) platform and (4) unilateral request by customers.

Inhaltsübersicht

I. Einleitung

Unter Open Finance[1] wird allgemein die Öffnung von Banken und Versicherungen[2] bzw. das Zur-Verfügung-Stellen eines Teils der durch sie bewirtschafteten Kundendaten gegenüber Drittanbietern (third party providers, [«TPPs»], z.B. FinTechs aber auch andere Banken) verstanden. Dabei werden via Schnittstelle (Application Programming Interface, [«API»[3]]) Daten auf Wunsch der Kundinnen und Kunden ausgetauscht und damit neue, innovative Dienstleistungen ermöglicht (z.B. die Möglichkeit, in einer App alle Bankkonten einer Person anzuzeigen[4] oder di-

* Prof. Dr. iur. *Cornelia Stengel,* Rechtsanwältin in Zürich, MLaw *Elena Rüegg,* wissenschaftliche Mitarbeiterin an der Fachhochschule Nordwestschweiz in Basel, Dr. iur. *Jessica Kim Sommer,* Rechtsanwältin, MLaw *Luca Stäuble,* Rechtsanwalt und MLaw *Benedikt Freund,* Rechtsanwalt, alle Zürich. Dieser Beitrag entstand im Rahmen des Gemeinschaftsprojekts «Collaboration Models – Enabling Open Finance» des #Fintank der Fachhochschule Nordwestschweiz, Swiss FinTech Innovations (SFTI) und der Schweizerischen Bankiervereinigung, welches vom Staatssekretariat für Internationale Finanzfragen SIF unterstützt wird.

1 Neben den klassischen und alltäglichen Banking Services, die beim Open Banking im Zentrum stehen, erfasst Open Finance auch Themen wie Sparen und Vorsorgesparen, Anlegen und Investieren, Hypotheken, Kredite, Versicherungen etc. (vgl. z.B. <*https://www.moneytoday.ch/lexikon/open-finance*> [zuletzt besucht: 12.1.2022]). – Vgl. auch die Definitionen bei *Rolf H. Weber,* Open Finance und Decentralized Finance – Entwicklungen in einem disruptiven Finanzmarktumfeld, SZW 2022, 3 ff., 3 f.

2 In der Folge ist jeweils bloss von der «Bank» die Rede, Versicherungen und andere Finanzintermediäre sind, wo zutreffend, auch mitgemeint.

3 Zur Definition von API siehe z.B. *David Roth,* «Open Banking» in der Schweiz – Herausforderungen an den Schnittstellen von Finanzmarkt-, Datenschutz- und Kartellrecht, SZW 2020, 669 ff., 670: «Plakativ formuliert ermöglicht eine API zwei Computeranwendungen, über ein Netzwerk in einer gemeinsamen Sprache zu kommunizieren. Dabei wird die API jeweils vom Dateninhaber zur Verfügung gestellt, welcher grundsätzlich zugleich die Zugriffskonditionen festlegt.» – Zur Erklärung und Unterscheidung der verschiedenen Öffnungsgrade der API vgl. *Andreas Imthurn,* Auswirkungen der PSD2-Regulierung auf die europäische Finanzindustrie unter besonderer Berücksichtigung der sogenannten «Open Banking APIs», Diss. Universität St. Gallen, St. Gallen 2021, 141.

4 Siehe z.B. die «Maximal-Variante» unter <*https://www.moneytoday.ch/lexikon/open-banking*> (zuletzt besucht: 12.1.2022). – Vgl. auch *Cornelia Stengel,* Open Banking verleiht Impulse, FuW vom 28. Oktober 2021, abrufbar

rekt aus einem Buchhaltungsprogramm Zahlungen auszulösen[5]).[6] Open Finance hat sich international vor allem durch regulatorische Vorgaben entwickelt.[7] Auch in der Schweiz sollen die Vorteile von Open Finance für Kundinnen und Kunden, Wirtschaft und Gesellschaft genutzt werden, wobei derzeit geprüft wird, ob dafür die regulatorischen Rahmenbedingungen anzupassen sind.[8]

Der vorliegende Aufsatz leistet hierzu einen Beitrag und untersucht anhand vier möglicher «Muster-Kooperationsformen» die rechtlichen Verhältnisse zwischen Bank, TPP, allenfalls Plattform sowie Kundinnen und Kunden. In der Praxis ist eine Vielzahl von Mischformen solcher Kooperationen anzutreffen, weshalb die hier dargestellten Konstellationen als Grundmodelle zu verstehen sind. Die nachfolgenden Ausführungen zeigen auf, wie die Kooperation zwischen den verschiedenen Akteuren im Bereich von Open Finance aussehen kann und wie sich die unterschiedlichen Formen auf die Haftung auswirken können.

Beispielhaft wird dies illustriert an der Frage der vertragsrechtlichen Haftung für Vermögensschäden (III) sowie den Fragen, gegen wen sich allfällige datenschutzrechtliche Ansprüche aus einem Datenschutzverstoss richten und wer einem entsprechenden Bussenrisiko ausgesetzt ist (IV).

Analysiert werden die Kooperationsformen *«Outsourcing», «gemeinsame Angebote»* von Banken und TPP, *«Plattform»* und *«einseitige Aufforderung»* von Kundinnen und Kunden.

II. Die vier Kooperationsformen

1. «Outsourcing»

Die Kooperationsform des *«Outsourcings»* (die Auslagerung einer Geschäftstätigkeit) liegt vor, wenn eine Bank einen Dienstleister beauftragt, selbständig und dauernd eine für die Geschäftstätigkeit des Unternehmens wesentliche Funktion ganz oder teilweise zu erfüllen.[9]

Obwohl beim Outsourcing ebenfalls Drittparteien involviert sind, ist diese Kooperationsform nicht dem Open Banking zuzuordnen, wie es im Allgemeinen verstanden wird. Im Falle des Outsourcings handelt der Dienstleister im Interesse und im Auftrag der Bank und nicht – wie bei Open Banking typisch – im Auftrag der Kundinnen und Kunden.[10] Um Unterschiede und Gemeinsamkeiten zu den Kooperationsformen von Open Banking darzustellen, wird im Folgenden dennoch punktuell auf diese klassische Form der Zusammenarbeit zwischen Banken und Drittanbietern eingegangen.

Die FINMA hat im Rundschreiben 2018/3 aufsichtsrechtliche Anforderungen an «Outsourcing»-Lösungen von Banken, Versicherungsunternehmen und ausgewählten Finanzinstituten festgelegt.[11] Dieses enthält namentlich Anforderungen an eine angemessene Organisation und bezweckt deren Risikobegrenzung.[12] Vorbehältlich Oberleitung, Aufsicht und Kontrolle durch das Oberleitungsorgan, zentrale Führungsaufgaben der Geschäftsleitung sowie Funktionen, die das Fällen von strategischen Entscheiden umfassen, ist die Auslagerung aller wesentlichen Funktionen grundsätzlich zulässig.[13]

Eine Auslagerung ermöglicht den Banken, beispielsweise im Bereich des Kunden-Onboardings, neueste Technologien einzusetzen, ohne diese selbst entwickeln zu müssen. Häufig sind die Dienstleister nicht unmittelbar in die IT-Infrastruktur der Bank eingebunden. Um die Dienstleistungen erbringen zu können, etwa das Auslösen von Zahlungseinlieferungen, benötigen die Dienstleister aber häufig Zugriff auf die Kundeninformationen. Die hierzu notwendi-

unter: <*https://www.fuw.ch/article/openbanking-verleiht-impulse/*> (zuletzt besucht: 12.1.2022).

5 Siehe z.B. <*https://www.bexio.com/de-CH/*> und <*https://www.six-group.com/de/newsroom/media-releases/2021/20211102-bexio-blink.html*> (zuletzt besucht: 12.1.2022).

6 Vgl. z.B. die Definitionen von Open Banking Project, abrufbar unter: <*https://www.openbankingproject.ch/en/resources/faq/*> oder Swiss Banking, abrufbar unter: <*https://www.swissbanking.ch/de/themen/digitalisierung-innovation-cyber-security/open-banking*> (zuletzt besucht: 12.1.2022). – Ähnlich auch *Stengel* (Fn. 4). – Siehe auch die Ausführungen bei *Weber* (Fn. 1), 3 f.

7 Vgl. Schweizerische Bankiervereinigung SBVg, Open Banking, Eine Auslegeordnung für den Schweizer Finanzplatz 2020, 3.

8 Vgl. *Stengel* (Fn. 4).

9 Angelehnt an die Definition nach dem FINMA-Rundschreiben 2018/3 «Outsourcing», Rz. 3.

10 SBVg (Fn. 7), 9.

11 FINMA-Outsourcing (Fn. 9), *passim.*

12 FINMA-Outsourcing (Fn. 9), Rz. 1.

13 FINMA-Outsourcing (Fn. 9), Rz. 7 f.

ge Kommunikation erfolgt in der Regel mittels bankinterner Schnittstelle – sogenannte interne API[14]. Dementsprechend findet der End-to-End-Prozess[15] einer ausgelagerten Dienstleistung in der Sphäre der Bank statt.

2. «Gemeinsame Angebote»

Bei der Kooperationsform des *«gemeinsamen Angebots»* kann das Zusammenwirken zwischen Bank und TPP sehr unterschiedlich intensiv ausfallen. Denkbar ist eine Kooperation, die von einem blossen Werben bis hin zu einem eigentlichen Ökosystem, bestehend aus verschiedenen TPPs reicht.[16] Typischerweise erhält auch beim *«gemeinsamen Angebot»* der TPP mittels bankinterner Schnittstelle bzw. API Zugriff auf die Kundeninformationen, die von der Bank bearbeitet und bereitgestellt werden, um seine Dienstleistung zu erbringen.

Ein wesentliches Merkmal dieser Kooperationsform ist der gemeinsame Auftritt bzw. eben das gemeinsame Angebot von Bank und TPP an die Kundinnen und Kunden. So können sowohl die Bank als auch der TPP eine «Open Banking-Dienstleistung» bewerben und anbieten, welche in dieser Form nur dank der Kooperation der beiden überhaupt erbracht werden kann.

In der Praxis finden sich bereits zahlreiche Angebote, die dem Kooperationsmodell «gemeinsame Angebote» entsprechen. Zu erwähnen sind die Buchhaltungssoftwares bexio[17] oder KLARA[18].[19] Hier wird die Software des TPP direkt mit dem Bankkonto der Kundinnen und Kunden verknüpft, sodass Zahlungen unmittelbar aus der Buchhaltungssoftware ausgelöst werden können und Zahlungseingänge sofort darin ersichtlich sind. Im Bereich der Wealth Management Systeme, welche insbesondere den Vermögensverwaltungsbereich betreffen, haben sich ebenfalls bereits Angebote etabliert, zu nennen sind z.B. Assetmax[20], Etops[21] oder Alphasys[22].[23] Ein weiteres Praxisbeispiel stellt das Modell (zumindest in seiner Anfangsform) der Hypothekarbank Lenzburg dar. Sie hat als erste Schweizer Bank ihre Schnittstelle bzw. API gegenüber verschiedenen Drittanbietern mittels der Finstar-Plattformtechnologie[24] geöffnet.[25] TPPs können sich mit ihren eigenen Softwaremodulen an der Plattform anschliessen,[26] womit die Hypothekarbank Lenzburg den Kundinnen und Kunden eine erweiterte Palette an Dienstleistungen anbieten kann, ohne bereits auf dem Markt bestehende Innovationen kopieren zu müssen.[27] Die Anbindung von einer grossen Anzahl Marktteilnehmenden an die Bank wird auch als «Ökosystem» bezeichnet.[28]

3. «Plattform»

Grundsätzlich liegt beim *«Plattformmodell»* eine ähnliche Konstellation vor wie schon beim *«gemeinsamen Angebot»*. Der Unterschied besteht darin, dass sich die Plattform zwischen die Bank und den TPP «schaltet» und als Intermediär oder auch «Verbindungsstück»

14 Vgl. dazu *Imthurn* (Fn. 3), 141: Auch private Schnittstellen bzw. APIs genannt. Die Daten sind nur dem Ersteller und bestimmten Parteien, basierend auf einer vertraglichen Grundlage, frei zugänglich.

15 Ein von den Kundinnen und Kunden ausgehender Prozess, der über verschiedene Abteilungen, oder gar Unternehmen, bis zur Erfüllung des gewünschten Resultats führt (vgl. *<https://www.wemakefuture.com/automatisierung/end-to-end-geschaftsprozesse>* [zuletzt besucht: 12.1.2022]).

16 Vgl. auch das Zusammenarbeitsmodell «Partnership model» nach PwC, The Future of Banking is Open, 2018, 45 f.

17 Siehe *<https://www.bexio.com/de-CH/>* (zuletzt besucht: 12.1.2022).

18 Siehe *<https://www.klara.ch/>* (zuletzt besucht: 12.1.2022).

19 Diese beiden Unternehmen haben sich unterdessen zudem an die Plattform bLink angeschlossen (siehe dazu: *<https://www.six-group.com/de/newsroom/media-releases/2020/20200519-six-blink.html>; <https://www.six-group.com/de/newsroom/media-releases/2021/20211102-bexio-blink.html>* [zuletzt besucht: 12.1.2022]).

20 Siehe *<https://www.assetmax.ch/>* (zuletzt besucht: 12.1.2022).

21 Siehe *<https://www.etops.ch/>* (zuletzt besucht: 12.1.2022).

22 Siehe *<https://www.alphasys.ch/de/>* (zuletzt besucht: 12.1.2022).

23 Diese Unternehmen sind ebenfalls an die Plattform bLink angeschlossen (vgl. dazu: *<https://www.six-group.com/de/blog/2021/open-wealth-standards.html>* [zuletzt besucht: 12.1.2022]).

24 Finstar ist eine von der Hypothekarbank Lenzburg entwickelte Kernbankensoftware, vgl. *<https://www.finstar.ch/de/produkte/>* (zuletzt besucht: 12.1.2022).

25 Vgl. *Marianne Wildi,* Open Banking, in: Susan Emmenegger (Hrsg.), Zahlungsverkehr, Bern 2018, 1 ff., 2.

26 Vgl. Finstar-Trailer, abrufbar unter: *<https://www.finstar.ch/de/produkte/>* (zuletzt besucht: 12.1.2022).

27 Vgl. *Wildi* (Fn. 25), 8.

28 Siehe z.B. *Wildi* (Fn. 25), 6 ff.

standardisierte Schnittstellen bzw. APIs bereitstellt – z.B. zur Vornahme von Zahlungseinlieferungen und zum Austausch von Kontoinformationen.[29]

Die Funktionsweise des *«Plattformmodells»* wird nachfolgend am Beispiel der von der SIX betriebenen Plattform bLink kurz skizziert. bLink bietet Banken und TPPs standardisierte Schnittstellen bzw. APIs, ein einheitliches Vertragswerk und standardisierte Zulassungsprüfungen an.[30] Um Zugriff auf die Schnittstellen bzw. APIs von bLink zu erhalten, müssen Banken und TPPs sich an die Plattform anschliessen und mit dieser eine vertragliche Vereinbarung («Teilnahmevertrag»[31]) abschliessen. Für die Aufnahme von TPPs sieht bLink eine Zulassungsprüfung vor, welche neben einer generellen Prüfung (HR-Eintrag, Sanktionslisten, unethischer Unternehmenszweck, nachhaltiger Business Plan) einen IT-Sicherheitsnachweis verlangt und prüft, dass die Daten für den vereinbarten Zweck verwendet werden.[32] Durch dieses «Zulassungsverfahren» trifft die Plattformbetreiberin gewissermassen eine Auswahl und bestimmt damit das «Marktangebot», welches den angeschlossenen Plattformnutzern offensteht.

Mit dem Anschluss an die Plattform findet allerdings – jedenfalls im Falle von bLink – kein automatischer Datenaustausch statt. Vielmehr schliessen die Plattformnutzer (Banken und TTPs) nach eigenem Entscheid[33] mit den ihnen zusagenden Partnern in einem weiteren Schritt einen zusätzlichen Vertrag («Anwendungsvertrag»[34]), wodurch die Bank ihre Angebotspalette erweitert. Dadurch erst kann der jeweilige TPP seine Dienstleistung den jeweiligen Bankkundinnen und -kunden anbieten.

Möchte schliesslich eine Kundin oder ein Kunde die «Open Banking-Dienstleistung» eines mit der Bank vertraglich verbundenen TPP in Anspruch nehmen, wird ein Vertrag zwischen Kundinnen und Kunden und TPP abgeschlossen. Selbstverständlich besteht immer auch ein Vertrag zwischen Kundinnen und Kunden und der Bank. Die Plattformbetreiberin und die Kundinnen und Kunden schliessen hingegen keinen Vertrag ab.

4. «Einseitige Aufforderung»

Kundinnen und Kunden fordern bei diesem Kooperationsmodell ihre Bank einseitig auf, einem TPP Zugriff auf ihre Kundeninformationen zu gewähren oder diesem sogar die Vornahme selbständiger Handlungen, wie beispielweise Zahlungen auszulösen, zu erlauben. Diese Kooperationsform beschreibt die regulatorisch verordnete Situation in der EU,[35] welche bislang allerdings einen beschränkten Anwendungsbereich hat. Im Idealfall werden bei diesem Kooperationsmodell standardisierte Schnittstellen bzw. APIs verwendet, mit denen die Bank – je nach Aufforderung der Kundin oder des Kunden – festlegen kann, welche Informationen der TPP erhalten und welche Funktionen er bedienen können soll.[36]

In der Schweiz unterliegen Banken keiner regulatorischen Pflicht, TPPs via (standardisierter) Schnittstelle bzw. API Zugriff auf Kundeninformationen zu gewähren.[37] Weigert sich eine hiesige Bank, diesen Zugriff zu gestatten bzw. verfügt sie über keine (standardisierte) Schnittstelle bzw. API, sieht die Kundin oder der Kunde sich gezwungen, dem TPP einen direkten Onlinezugriff auf ihr/sein Konto einzuräumen, indem etwa die PIN oder die Transaktionsnummer weitergegeben werden.[38] Durch die Weitergabe der Identifikationsmittel kann der TPP sodann ohne Schranken alle Kundendaten, welche die Bank zur

29 Vgl. dazu *Roth* (Fn. 3), 673 ff.

30 Siehe *<https://www.six-group.com/de/products-services/banking-services/blink.html#scrollTo =was_hat_blink_mitopenbankingzutun>; <https://www.six-group.com/de/products-services/banking-services/blink.html#scrollTo=welche_dienstleistungenanwendungenbietet blink>* (zuletzt besucht: 12.1.2022).

31 Vgl. Teilnahmebedingungen bLink Plattform, Rz. 5.

32 Siehe dazu *<https://www.six-group.com/de/products-services/banking-services/blink.html#scrollTo=was_wird_bei_derzulassungspruefunggeprueft>* (zuletzt besucht: 12.1.2022).

33 Vgl. dazu Teilnahmebedingungen (Fn. 31), Rz. 39.

34 Vgl. Teilnahmebedingungen (Fn. 31), Rz. 44.

35 Siehe zur Richtlinie sogleich unten.

36 Vgl. *Imthurn* (Fn. 3), 139, der von der Freigabe nur der gewünschten Funktionen und Daten spricht.

37 Anstelle vieler *Marco Birkhofer/Sandro Bächli,* Open Banking und standardisierte Schnittstellen auf dem Finanzplatz Schweiz, in: Jochen Schellinger/Kim Oliver Tokarski/Ingrid Kissling-Näf (Hrsg.), Digital Business, Bern 2020, 119 ff., 124. – Vgl. auch *Stengel* (Fn. 4).

38 *Susan Emmenegger,* Die EU öffnet den Markt für neue Zahlungsdienstleister, Die Volkswirtschaft vom 24. Mai 2018, abrufbar unter: *<https://dievolkswirtschaft.ch/de/2018/05/die-eu-oeffnet-den-markt-fuer-neue-zahlungsdienstleister/#:~:text=Die%20Digitalisierung%20f%C3%BChrt%20auf%20dem, auf%20die%20Konten%20von%20Bankkunden>* (zuletzt besucht: 12.1.2022).

betreffenden Kundin oder zum betreffenden Kunden bearbeitet, einsehen und die im Onlinebanking vorhandenen Funktionen nutzen, um seine eigene Dienstleistung, wie beispielsweise die Übersicht über Guthaben bei verschiedenen Banken der Kundin oder des Kunden erstellen oder auch direkt eine Zahlung auslösen.[39] Diese Methode hat allerdings insbesondere unter Sicherheitsaspekten bedeutende Nachteile, da Kundinnen und Kunden ihre eigenen Identifikationsmittel an Dritte bekanntgeben, die in der Schweiz keiner spezifischen regulatorischen Kontrolle unterstehen.[40] Problematisch ist zudem, dass die meisten Schweizer Banken in ihren AGB den Kundinnen und Kunden die Weitergabe der Identifikationsmittel verbieten bzw. deren sorgfältige Aufbewahrung vorschreiben.[41]

Im Gegensatz zur Schweiz sind die Banken innerhalb der EU aufgrund der PSD2-Verordnung[42] verpflichtet, einem TPP auf Wunsch ihrer Kundinnen und Kunden über eine separate Schnittstelle bzw. API Zugriff auf die Kundeninformationen zu gewähren («Kontoinformationsdienst») oder diesem zu ermöglichen, dass er Zahlungen via Kundenkonto gleich schnell und zu denselben Kosten selbständig auslösen kann, wie wenn die Bank diese selbst vorgenommen hätte («Zahlungsauslösedienst»). Dies ermöglicht z.B. die Auskunft an einen Händler, ob das Konto der betreffenden Kundin bzw. des betreffenden Kunden, die/der dem TPP die Erlaubnis zur Abfrage erteilt hat, über den notwendigen Betrag für einen Online-Kauf verfügt.[43]

III. Vertragsrechtliche Haftung für Vermögensschäden

1. Rechtliche Erfassung der Kooperationsformen

1.1 «Outsourcing»

Die Bank bedient sich beim «*Outsourcing*» für die Erfüllung der eigenen Leistungspflicht gegenüber den Kundinnen und Kunden eines Dritten, ohne dass dieser einen Vertrag mit den Kundinnen und Kunden abschliesst. Bei den ausgelagerten Pflichten steht in der Regel die auftragsrechtliche Komponente des Bankvertrags im Vordergrund (Art. 394 ff. OR). Für das Verhalten des Dienstleisters hat die Bank grundsätzlich nach den Regeln der Hilfspersonenhaftung (Art. 101 OR) – allenfalls qualifiziert der Dienstleister als Substitut (Art. 398 Abs. 3 und Art. 399 OR) – einzustehen.[44]

Obwohl gemäss FINMA-Rundschreiben wesentliche Funktionen ganz oder teilweise selbständig durch Dritte erledigt werden können,[45] was für Substitution spräche, muss unternehmensintern eine verantwortliche Stelle definiert werden, die für die laufende Überwachung und Kontrolle sorgt und sich vertraglich die dafür notwendigen Weisungs- und Kontrollrechte einräumen lässt.[46] Ausserdem trägt das auslagernde Unternehmen gegenüber der FINMA dieselbe Verantwortung, wie wenn es die ausgelagerte Funktion selbst erbringen würde.[47] Diese Umstände sprechen vielmehr für die Qualifikation des Dienstleisters als Hilfsperson i.S.v. Art. 101 OR.[48]

39 Vgl. *Jana Essebier/Janique Bourgeois,* Open Banking – Der Zahlungsverkehr im Umbruch, EuZ 2018, 116 ff., 120; *Stengel* (Fn. 4).

40 *Roth* (Fn. 3), 684 m.w.H.; *Emmenegger* (Fn. 38).

41 Vgl. *Emmenegger* (Fn. 38).

42 Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG, ABl 2015 L 337/35.

43 *Imthurn* (Fn. 3), 72.

44 Bei der Unterscheidung wird relevant, in wessen Interesse der Beizug einer Drittperson erfolgt (Interessenlage) und ob die geschuldete Leistung weisungsgebunden und unter Aufsicht erbracht wird (Selbständigkeit). Zu den Unterscheidungskriterien siehe z.B. *Walter Fellmann,* in: Heinz Hausheer (Hrsg.), Berner Kommentar zum schweizerischen Privatrecht, Art. 394–406 OR. Der einfache Auftrag, Bern 1992 (zit. BK-*Autor/in*), Art. 398 N 535 ff.; BGer 4A_407/2007 vom 14.3.2008 E. 2.3.

45 FINMA-Outsourcing (Fn. 9), Rz. 3; SBVg (Fn. 7), 9.

46 FINMA-Outsourcing (Fn. 9), Rz. 20 f.

47 FINMA-Outsourcing (Fn. 9), Rz. 23.

48 Ähnlich, aber mit anderer Begründung, *Martin Hess,* Die Haftung der Banken für Kundendatendiebstahl, in: Susan Emmenegger (Hrsg.), Bankhaftungsrecht, Bern 2006, 55 ff., 85.

1.2 «Gemeinsame Angebote»

Verglichen mit der Kooperationsform des *«Outsourcings»* stehen den Kundinnen und Kunden beim *«gemeinsamen Angebot» zwei* Vertragsparteien gegenüber – die Bank und der TPP. Die den Kundinnen und Kunden *gemeinsam* vertraglich versprochene Leistung kann beim gemeinsamen Angebot sehr unterschiedlich ausgestaltet sein. Vorstellbar ist, dass sich diese auf die *Abwicklung* der «Open Banking-Dienstleistung» über die Schnittstelle bzw. API beschränkt und deshalb insbesondere die Leistungspflicht hinsichtlich des *Gegenstands* der «Open Banking-Dienstleistung» (z.B. Buchhaltungssoftware) beim TPP verbleibt. Je nach Intensität der Zusammenarbeit kann aber auch der *Gegenstand* der «Open Banking-Dienstleistung» gemeinsam von TPP und Bank geschuldet sein.

In der Regel wird dieses Vertragsverhältnis betreffend die gemeinsame Leistung (gemeinsame Abwicklung oder auch gemeinsam geschuldete «Open Banking-Dienstleistung) schwergewichtig den auftragsrechtlichen Regeln unterstehen (Art. 394 ff. OR).

Je nachdem, welche Bedeutung dem kooperativen Element zwischen Bank und TPP zukommt, kann eine gemeinschaftliche Übernahme eines Auftrags oder auch eine einfache Gesellschaft vorliegen.[49] In beiden Fällen sieht das Gesetz eine solidarische Haftung der Beauftragten gegenüber dem Auftraggeber vor (Art. 403 Abs. 2 und Art. 544 Abs. 3 OR).[50]

Bei der gemeinschaftlichen Übernahme eines Auftrags ist sowohl vorstellbar, dass die Parteien *einen* Vertrag abschliessen, wie auch dass die Kundinnen und Kunden *separate* Verträge mit Bank und TPP vereinbaren. Diese unterschiedliche Ausgestaltung hat auf die Haftung keinen Einfluss, denn trifft nur einen Beauftragten ein Verschulden, so hat er auch bei der Annahme eines einheitlichen Vertragsverhältnisses grundsätzlich allein für den Schaden einzustehen (Art. 398 Abs. 2 i.V.m. Art. 97 Abs. 1 OR).[51] Zu bedenken bleibt, dass oftmals eine Vertragsverletzung auf dem Unterlassen des anderen Beauftragten gründet, was wiederum ein gemeinsames Verschulden (i.S.v. Art. 50 Abs. 1 OR) darstellen und Solidarhaftung zur Folge haben könnte.[52] Zudem können vor allem die Bank aus dem unterliegenden Bankvertrag auftragsrechtliche Sorgfaltspflichten treffen, die eine generelle Wahrung der Interessen der Kundinnen und Kunden verlangen.[53]

1.3 «Plattform»

Wie beim *«gemeinsamen Angebot»* bieten auch beim *«Plattformmodell»* die Bank und der TPP den Kundinnen und Kunden gemeinsam eine Dienstleistung (von der blossen gemeinsamen Abwicklung bis zur gemeinsamen «Open Banking-Dienstleistung») an, für welche diese grundsätzlich den Kundinnen und Kunden solidarisch haften (vgl. dazu zuvor Ziff. III.1.2). Zusätzlich wird beim *«Plattformmodell»* bei der Erbringung der Dienstleistung die Plattform «zwischengeschaltet». Regelmässig – so z.B. bei bLink – besteht zwischen Kundinnen und Kunden und Plattformbetreiberin kein Vertragsverhältnis.[54]

Die Plattform ist als Hilfsperson (Art. 101 OR) – oder allenfalls Substitutin (Art. 398 Abs. 3 und Art. 399 OR) – sowohl der Bank wie auch des TPP zu qualifizieren. Für die Annahme einer Hilfsperson spricht, dass die Plattform nicht primär im Interesse der Kundinnen und Kunden beigezogen wird – allenfalls wissen diese nicht einmal davon –, sondern der Beizug der Erleichterung der Abwicklung der Dienstleistung dient. So wäre eine Erbringung der Dienstleistung – wie beim *«gemeinsamen Angebot»* – auch ohne Plattform möglich. Im Zusammenhang mit Vermögensschäden ist deshalb zu prüfen, inwiefern die Bank bzw. der TPP für das Verhalten der Plattformbetreiberin gegenüber den Kundinnen und Kunden einzustehen haben (Hilfsperson/Substitutin).

1.4 «Einseitige Aufforderung»

Im Kooperationsmodell *«einseitige Aufforderung»* bestehen regelmässig Vertragsverhältnisse zwischen der Bank und den Kundinnen und Kunden und zwischen Kundinnen und Kunden und TPP. Zwischen Bank und TPP besteht meistens keine vertragliche Beziehung, sondern deren Kontakt erfolgt aufgrund

[49] Vgl. BK-*Fellmann* (Fn. 44), Art. 403 N 26 ff.; *Urs Egli,* Forschungs- und Entwicklungsverträge: zentrale Rechtsfragen und Hinweise zur Vertragsgestaltung, AJP 2015, 993 ff., 994, im Hinblick auf F&E Verträge.

[50] BK-*Fellmann* (Fn. 44), Art. 403 N 30.

[51] BK-*Fellmann* (Fn. 44), Art. 403 N 158 ff., N 162 ff. – Siehe aber nachfolgend zur Schadensabwälzung bei Legitimationsmängeln (Ziff. III.3).

[52] BK-*Fellmann* (Fn. 44), Art. 403 N 163.

[53] Siehe die nachfolgenden Ausführungen zur Verantwortlichkeit der Bank für das Verhalten des TPP (Ziff. III.4).

[54] Vgl. Teilnahmebedingungen (Fn. 31), Rz. 48.

des Wunsches der Kundin bzw. des Kunden. Die durch den Bankvertrag generell beauftragte Bank führt demnach eine Weisung ihrer Kundin bzw. ihres Kunden aus (Art. 397 Abs. 1 OR).[55] Handelt es sich beim Auftrag um eine Zahlung, liegt regelmässig eine Anweisung vor, die vom TTP als Stellvertreter der Kundin bzw. des Kunden ausgelöst wird (Art. 466 ff. und Art. 32 ff. OR).

2. Fragestellung

Im Folgenden wird einerseits untersucht, wer für den Vermögensschaden infolge eines Legitimationsmangels (z.B. «Man-in-the-Middle»-Attacke) vertragsrechtlich verantwortlich ist (Ziff. III.3). Andererseits wird die Situation analysiert, in welcher Kundinnen und Kunden aufgrund eines sorgfaltswidrigen Verhaltens des TPP (z.B. eine nicht dem Risikoprofil angepasste Anlageempfehlung) einen Vermögensschaden erleiden (Ziff. III.4).

3. Legitimationsmängel («Man-in-the-Middle»-Attacke)

3.1 Ausgangslage

Werden Transaktionen via Schnittstelle bzw. API durchgeführt, so besteht nicht nur eine direkte Kommunikationslinie zwischen der Bank und den Kundinnen und Kunden, sondern es werden Dritte – TPPs – miteinbezogen. Indem weitere Akteure bei der Transaktion mitwirken, entsteht durch diese zusätzlichen Angriffspunkte ein grösseres Risiko beispielsweise für Auszahlungen an unbefugte Dritte aufgrund von «Man-in-the-Middle»-Attacken.[56]

Kommt ein Dritter z.B. mittels *Phishing*[57] an die Legitimationsmittel der Kundinnen und Kunden und manipuliert er anhand dieser einen Zahlungsauftrag an der Schnittstelle bzw. API (z.B. «Man-in-the-Middle»-Attacke), entsteht den Kundinnen und Kunden ein Vermögensschaden. Diese Situation entspricht den Fällen, bei welchen die Bank unautorisierte Zahlungen aufgrund einer Täuschung vornimmt («Legitimationsmängel»[58]).

Für die Frage, wer den aufgrund von Legitimationsmängeln entstandenen Schaden tragen muss, hat das Bundesgericht ein dreistufiges Prüfschema entwickelt.[59] In einem *ersten Schritt* prüft das Bundesgericht, ob die fragliche Zahlung mit oder ohne Anweisung der Kundin/des Kunden erfolgte. Mangelt es an einer Anweisung, trägt die Bank den Schaden und der Erfüllungsanspruch der Kundin bzw. des Kunden bleibt bestehen (Ziff. III.3.2). Ist dies der Fall, prüft das Bundesgericht in einem *zweiten Schritt,* ob die Parteien eine gültige Schadensabwälzungs- oder Risikoüberwälzungsklausel vereinbart haben und die Bank gestützt darauf den Schaden überwälzen kann (Ziff. III.3.3). Wurde keine Schadensabwälzung vereinbart, prüft das Bundesgericht in einem *dritten Schritt,* ob die Bank den Erfüllungsanspruch mit einem Schadenersatzanspruch gegenüber den Kundinnen und Kunden verrechnen kann (Ziff. III.3.4).

Im Folgenden werden die einzelnen Schritte kurz skizziert und aufgezeigt, welche Bedeutung diesen in den verschiedenen Kooperationsformen zukommen kann.

3.2 Zahlung mit oder ohne Anweisung (erster Schritt)

Zwischen Bank und Kundinnen und Kunden besteht ein Kontovertrag. Dieser wird in der Lehre als Darlehensvertrag oder irregulärer Hinterlegungsvertrag

55 Vgl. z.B. BGE 110 II 283 E. 1.

56 Bei einer «Man-in-the-Middle»-Attacke schiebt sich ein «Angreifer» unbemerkt, meistens mittels Software, «in die Mitte» zweier oder mehrerer Kommunikationspartner mit dem Ziel, Vermögenswerte auf ein eigenes Konto umzuleiten. Zuerst gibt er sich dem Sender gegenüber als Empfänger aus, um die Datenpakete auf ein Drittsystem umzuleiten. Je nach Ausgangslage analysiert und verändert er sodann die Datenpakete und leitet diese anschliessend unter der Vorspiegelung, der wirkliche Sender zu sein, dem eigentlichen Empfänger weiter (vgl. Beschluss der BKartA-Beschl. B4-71/10 vom 29.6.2016, Rz. 53 Fn. 39; *Susan Emmenegger,* Unautorisierte Transaktionen im Zusammenhang mit Dritten Zahlungsdienstleistern, in: Susan Emmenegger (Hrsg.), Zahlungsverkehr, Bern 2018, 87 ff., 93 f.; *Peter Reichart,* Betrugsversuche im Zahlungsverkehr im digitalen Zeitalter, SZW 2019, 392 ff., 393).

57 *Jean-Marc Schaller,* Legitimationsmängel, in: Susan Emmenegger (Hrsg.), Bankvertragsrecht, Bern 2017, 45 ff., 59 f.

58 Siehe eine Übersicht zu den unterschiedlichen Arten bei *Schaller* (Fn. 57), 49 ff.

59 Siehe z.B. BGE 146 III 121; 146 III 326. – Dazu auch *Susan Emmenegger/Luc Thévenoz/Martina Reber/Célian Hirsch,* Das schweizerische Bankprivatrecht 2020, SZW 2021, 192 ff., 197.

mit auftragsrechtlichen Elementen qualifiziert.[60] Das Kontoguthaben stellt dabei eine Forderung der Kundinnen und Kunden gegenüber der Bank dar, die bei ordnungsgemässer Erfüllung – durch Verrechnung – erlöscht.[61] Leistet die Bank auf Anweisung der Kundinnen und Kunden an einen Dritten, erhält diese gegenüber den Kundinnen und Kunden einen Rückerstattungsanspruch (Verwendungsersatz, Art. 402 OR), welchen sie mit dem Erfüllungsanspruch verrechnen kann. Eine Überweisung *ohne* Anweisung der Kundinnen und Kunden lässt keinen entsprechenden Rückerstattungsanspruch entstehen.[62] Bei der Frage, ob die Zahlung mit oder ohne Anweisung erfolgte, wird insbesondere das Stellvertretungsrecht relevant (Art. 32 ff. OR).[63]

Leistet die Bank *ohne* Anweisung der Kundinnen und Kunden an einen Dritten, so haftet sie nach der gesetzlichen Regelung grundsätzlich – auch ohne Verschulden – für den entstandenen Schaden, und der Erfüllungsanspruch der Kundinnen und Kunden bleibt bestehen.[64] Haben die Parteien keine Schadensabwälzungs- oder Risikoübertragungsklausel vereinbart, darf der Erfüllungsanspruch der Kundinnen und Kunden nicht aufgrund von Selbst- oder Mitverschulden nach Art. 44 Abs. 1 i.V.m. Art. 99 Abs. 3 OR reduziert werden.[65] Bei Selbst- oder Mitverschulden der Kundinnen und Kunden muss die Bank einen separaten Schadenersatzanspruch gegen diese gestützt auf Vertragsverletzung (z.B. vertragswidrige Aufbewahrung der PIN) oder Delikt geltend machen (vgl. Ziff. III.3.4).[66]

Erlischt der Erfüllungsanspruch der Kundinnen und Kunden, weil von einer Zahlung *mit* Anweisung ausgegangen wird (z.B. weil die Kontoauszüge aus Unvorsicht genehmigt wurden), ist der Schaden aber auf ein Verschulden der Bank zurückzuführen (z.B. ungenügende Sicherung der Schnittstelle bzw. API), stellt sich die Frage, ob die Kundinnen und Kunden eine Schadenersatzklage gegenüber der Bank geltend machen können (Art. 398 Abs. 2 i.V.m. Art. 97 Abs. 1 OR).[67]

Für alle Kooperationsformen kann festgehalten werden, dass zwischen der Bank und den Kundinnen und Kunden ein Kontovertrag besteht. Leistet die Bank aufgrund eines Legitimationsmangels *ohne* Anweisung an einen Dritten, so trägt nach der gesetzlichen Regelung in diesem *ersten Schritt* die Bank den Schaden (Erfüllungsanspruch aus Kontovertrag bleibt bestehen, Rückforderungsanspruch gestützt auf Art. 402 OR entsteht nicht). Über eine Verteilung dieses Schadens im Innenverhältnis kann die Bank mit dem TPP Vereinbarungen treffen. Einzig im Modell der *«einseitigen Aufforderung»* besteht diese Möglichkeit in der Grundform nicht, da dort kein Vertragsverhältnis zwischen Bank und TPP besteht.

3.3 Schadensabwälzungs- oder Risikoübertragungsklausel (zweiter Schritt)

Muss die Bank aufgrund eines Legitimationsmangels doppelt zahlen – einmal an den nicht berechtigten Dritten und einmal an die Kundin bzw. den Kunden (Erfüllungsanspruch) –, erleidet die Bank einen Schaden und nicht die Kundin oder der Kunde.[68] Üblicherweise wird dieser Schaden mittels Schadensabwälzungs- oder Risikoübertragungsklauseln an die Kundinnen und Kunden weitergereicht.[69] Die Rechtsnatur dieser Klauseln und die darauf anzuwendenden Schranken sind Gegenstand von Diskussionen in der Lehre.[70] Das Bundesgericht wendet bei den Schadensabwälzungs- und Risikoübertragungsklauseln

60 Vgl. *Schaller* (Fn. 57), 46 ff.; *Reichart* (Fn. 56), 393 f., beide m.w.H.

61 *Schaller* (Fn. 57), 46 f.

62 BGE 146 III 121 E. 3.1.2 m.w.H. – Vgl. auch *Fabien Liégeois/Célian Hirsch,* Ordres bancaires frauduleux: discours de la méthode, SJ 2021, 117 ff., 124; *Nicolas Bracher,* Legitimationsprüfung und Risikotransfer bei E-Mail-Zahlungsaufträgen, SZW 2018, 156 ff., 157.

63 Siehe z.B. BGE 146 III 121 E. 3.2. – Dazu ausführlich auch *Liégeois/Hirsch* (Fn. 62), 125 ff.

64 BGE 146 III 121 E. 3.1.2; 146 III 387 E. 3.2, beide m.w.H.

65 Dieser Reduktionsgrund ist nach Rechtsprechung des BGer nur auf Schadenersatzansprüche anwendbar (BGE 146 III 387 E. 3.2 m.w.H.; siehe auch *Reichart* [Fn. 56], 394).

66 BGer 4A_504/2018 vom 10.12.2019 E. 5.1; *Reichart* (Fn. 56), 399 f.; *Sandro Bernet/Hans Caspar von der Crone,* Haftungsrechtliche Stellung der Bank bei Vollmachtsverhältnissen, Bundesgerichtsurteil 4A_504/2018 vom 10. Dezember 2019 (BGE 146 III 121), SZW 2020, 489 ff., 499 f.; *Bracher* (Fn. 62), 158.

67 Vgl. BGE 146 III 387 E. 3.2.

68 BGE 146 III 121 E. 4.1; 146 III 387 E. 5.1.

69 Vgl. BGE 146 III 326 E. 6.1. – Siehe auch *Liégeois/Hirsch* (Fn. 62), 129 ff.; *Bracher* (Fn. 62), 158.

70 *Susan Emmenegger/Luc Thévenoz/Thirza Döbeli/Leandro Lepori,* Das schweizerische Bankprivatrecht 2016, SZW 2017, 210 ff., 221; *Markus Vischer,* Schadensabwälzungsklauseln, Urteilsbesprechung 4A_379/2016 vom 15. Juni

die Schranke von Art. 100 Abs. 1 OR (kein Ausschluss bei Grobfahrlässigkeit) ohne dogmatische Begründung *analog* an.[71] In jüngster Zeit hat das Bundesgericht Art. 100 Abs. 2 OR (kein Ausschluss für leichte Fahrlässigkeit nach gerichtlichem Ermessen) auf Schadensabwälzungs- und Risikoübertragungsklauseln nicht mehr – wie bis anhin – analog angewendet.[72] Im Hinblick auf den Ausschluss der Haftung für höchstens leichtes Verschulden im Zusammenhang mit Hilfspersonen ist daher unklar, ob das Bundesgericht weiterhin Art. 101 Abs. 3 OR zur Anwendung bringt.[73]

Ist das Verhalten der Bank folglich als nicht grobfahrlässig einzustufen, kann sie den aufgrund des Legitimationsmangels entstandenen Schaden auf die Kundinnen und Kunden abwälzen. Gemäss Bundesgericht sind davon sogar Schäden erfasst, die sich durch Zufall ereignen.[74] Das Bundesgericht hat aber wohl im Sinne einer Zuteilung nach Risikosphären präzisiert, dass eine Kundin oder ein Kunde zwar den durch Zufall (ohne ihr/sein Verschulden) entstandenen Schaden aufgrund eines Hackerangriffs auf ihre/seine Mailbox zu tragen habe, sofern aber das Informatiksystem der Bank gehackt worden sei, etwas anderes gelte.[75] Unklar bleibt somit, ob das Bundesgericht damit eine Überwälzung von Zufällen in der Risikosphäre der Bank auf die Kundinnen und Kunden als nicht (mehr) zulässig erachtet.[76]

Es stellt sich die Frage, wann die Bank im Zusammenhang mit via Schnittstellen bzw. APIs abgewickelten unautorisierten Transaktionen ein grobes Verschulden treffen könnte. Wie bei klassischen Anweisungsverhältnissen löst auch bei Open Banking Konstellationen eine Kundin bzw. ein Kunde – via TPP – eine Zahlung bei der Bank via Anweisung aus. Der einzige Unterschied ist, dass bei dieser Transaktion die Schnittstellen bzw. APIs der Bank einem grösseren Manipulationsrisiko ausgesetzt sind, da technisch mehr Angriffspunkte entstehen, als wenn diese nur der Bank zugänglich sind. Aber auch wenn keine Öffnung der Schnittstellen bzw. APIs vorliegt, ist es möglich, dass die internen Schnittstellen bzw. APIs (Informatiksystem der Bank) gehackt werden.[77]

Der Bank obliegt in erster Linie die Pflicht, ihre Schnittstellen bzw. APIs genügend zu sichern.[78] Mit den fortschreitenden technischen Möglichkeiten erhöhen sich folglich auch die Anforderungen[79] an die Sicherheitsvorkehrungen.[80] Ist der Schaden auf eine mangelhafte Sicherung der Schnittstellen bzw. APIs zurückzuführen, so muss die Bank grundsätzlich dafür einstehen.[81] Hat sie die Schnittstellen bzw. APIs hingegen genügend gesichert und ist der Schaden der Risikosphäre der Kundin/des Kunden zuzuordnen, so darf sie davon ausgehen, dass der Schaden mittels Schadensabwälzungsklausel auf die Kundinnen und Kunden überwälzt werden darf.[82]

Festzuhalten bleibt: Die Bank ist in sämtlichen Kooperationsformen verpflichtet, genügende Sicherheitsvorkehrungen zu treffen. Gewährleistet die Bank diese Sicherheit, so handelt sie nicht grobfahrlässig, und eine Schadensabwälzung auf die Kundinnen und Kunden ist grundsätzlich möglich, sofern eine entsprechende Klausel (gültig) vereinbart wurde. Un-

2017, dRSK vom 8. September 2017, Rz. 22; *Bernet/von der Crone* (Fn. 66), 498 f.

71 Vgl. z.B. BGE 146 III 326 E. 6. – Siehe auch *Bracher* (Fn. 62), 158 und die Beispiele bei *Liégeois/Hirsch* (Fn. 62), 130 f.

72 So z.B. BGE 146 III 326 E. 4.2; siehe dazu *Emmenegger/Thévenoz/Reber/Hirsch* (Fn. 59), 199 f. m.w.H. und *Liégeois/Hirsch* (Fn. 62), 131.

73 Bis anhin wurde Art. 101 Abs. 3 OR angewendet: BGE 132 III 449 E. 2. – Dazu auch *Liégeois/Hirsch* (Fn. 62), 132.

74 BGE 146 III 326 E. 6.1; BGer 4A_379/2016 vom 15.6.2017 E. 3.3.1.

75 BGE 146 III 326 E. 6.3.2.3.

76 Vgl. *Reichart* (Fn. 56), 400 f., der sich für eine Aufteilung der Zufallshaftung nach Risikosphären ausspricht. Das Bundesgericht hat die Überbindung des Zufalls bis anhin grundsätzlich als zulässig erachtet (BGE 108 II 314 E. 2; BGer 4A_379/2016 vom 15.7.2017 E. 3.3.1). – Fraglich ist zudem, ob eine Schadensabwälzung der Haftung für Zufälle vor Art. 8 UWG standhält (siehe dazu auch *Reichart* [Fn. 56], 400 m.w.H.).

77 Vgl. BGE 146 III 326 E. 6.3.2.3.

78 *Reichart* (Fn. 56), 401: «Ohne weiteres kann vorausgesetzt werden, dass die Computersysteme der Bank, ihre Online-Banking-Tools sowie die Schnittstellen zum Computersystem des Kunden (bzw. des von diesem genutzten Drittanbieters) ‹sicher› sind.»

79 Siehe z.B. die Pflichten gemäss FINMA-Rundschreiben 2008/21 «Operationelle Risiken – Banken», Rz. 135 ff. zur Technologieinfrastruktur.

80 *Reichart* (Fn. 56), 401 m.w.H.: ‹‹Sicher› ist allerdings aufgrund der technischen Entwicklung ein wandelbarer Begriff. Sorgfaltswidrig verhält sich auf jeden Fall eine Bank, die ein System verwendet, das bei der Mehrzahl anderer Institute nicht mehr im Einsatz ist und hinter den Sicherheitsstandards von neueren Systemen zurückbleibt. Die Sicherheitsvorkehrungen müssen mithin *state of the art* sein».

81 Vgl. *Reichart* (Fn. 56), 400 f.

82 Vgl. *Reichart* (Fn. 56), 400 f.

klar ist, ob mit Blick auf die neuere bundesgerichtliche Rechtsprechung (und Art. 8 UWG) eine Abwälzung von Schäden, die aufgrund eines Zufalls in der Risikosphäre der Bank entstehen, gültig vereinbart werden kann.

Ist der Schaden im Modell *«Outsourcing»* auf mangelnde Sicherheitsvorkehrungen des Dienstleisters zurückzuführen,[83] ist dieses Verhalten auch basierend auf den entsprechenden Rundschreiben der FINMA immer der Risikosphäre der Bank zuzurechnen (Art. 101 OR).[84] Unklar ist, wie erwähnt, ob für die Wegbedingung der Haftung für Hilfspersonen Art. 101 Abs. 2 oder Abs. 3 OR zur Anwendung kommt.

Ereignet sich ein Schaden in der Kooperationsform des *«gemeinsamen Angebots»* oder im *«Plattformmodell»*[85] muss im Einzelfall beurteilt werden, in wessen Risikobereich – Bank oder Kundinnen und Kunden – sich eine Zuordnung rechtfertigt. Für die Zuordnung sind die Näheverhältnisse und vertraglichen Vereinbarungen zwischen den Parteien zu berücksichtigen. Sichert im *«Plattformmodell»* die Plattform ihre Schnittstelle bzw. API mangelhaft (oder ereignet sich durch Zufall ein Schaden), so ist dies dem Risikobereich der Bank zuzurechnen, weil sie die Plattform als Hilfsperson (Art. 101 OR) beizieht.[86]

Im Modell der *«einseitigen Aufforderung»* dürfte das Verhalten des TPP regelmässig dem Risikobereich der Kundinnen und Kunden zuzuordnen sein. Dies einerseits deshalb, weil die Kundinnen und Kunden den TPP selbst auswählen, und andererseits, da zwischen der Bank und dem TPP kein Vertragsverhältnis besteht.

Schliesslich stellt sich in diesem Zusammenhang die Frage, inwiefern Banken verpflichtet sind, die Transaktionen der Kundinnen und Kunden zu überwachen bzw. ob ein Unterlassen einer solchen Überwachung allenfalls als grobfahrlässig eingestuft werden könnte, womit eine Schadensabwälzung wiederum nicht zulässig wäre.[87] Bislang haben sich – ausserhalb der Bekämpfung von Geldwäscherei und Terrorismusfinanzierung – keine klaren Vorgaben etabliert, welche Massnahmen diesbezüglich von den Banken verlangt werden können (z.B. Geoblocking, Profiling, Regulatory Technical Standards der EU).[88] Diese Unsicherheit aus der Sicht der Bank erhält in Zusammenhang mit Open Banking jedoch keine zusätzliche Dimension. Sind unautorisierte Transaktionen aufgrund von Legitimationsmängeln erfolgt, so spielt es im Hinblick auf die Pflicht zur Überwachung der Transaktionen auf dem Konto der Kundinnen und Kunden keine Rolle, ob diese klassisch über Bankanweisungen – z.B. via Vertretung – erfolgen oder via (offene) Schnittstelle bzw. API ausgelöst werden.

3.4 Schadenersatzklage (dritter Schritt)

Haben die Parteien keine Schadensabwälzung vereinbart,[89] so prüft das Bundesgericht in einem dritten Schritt, ob die Bank dem Erfüllungsanspruch der Kundinnen und Kunden (vgl. Ziff. III.3.2) verrechnungsweise einen Schadenersatzanspruch (Art. 97 Abs. 1 oder Art. 41 Abs. 1 OR) entgegenhalten kann.[90]

Umstritten ist, ob dieser dritte Schritt auch geprüft wird, wenn die Parteien zwar eine Schadensabwälzung vereinbart haben, diese aber nicht zur Anwendung gelangt, weil z.B. das Verhalten der Bank grobfahrlässig ist. Je nach Lehrmeinung gilt in diesen Fällen die Schadenstragung als abschliessend geregelt («the buck stops here»[91]), oder die Bank kann den Erfüllungsanspruch mit Ansprüchen gegenüber den Kundinnen und Kunden – aufgrund (Mit-)Verschuldens – herabsetzen oder verrechnen.[92]

83 Oder ist der Schaden im Risikobereich des Dienstleisters durch Zufall eingetreten (z.B. Hackerangriff auf Dienstleister).

84 Dazu FINMA-Outsourcing (Fn. 9), Rz. 23 und FINMA-Operationelle Risiken – Banken (Fn. 79), Rz. 135 ff.

85 Z.B. ein Schaden ereignet sich aufgrund des Verhaltens des TPP (mangelhafte Sicherheitsvorkehrungen) oder durch Zufall (z.B. Hackerangriff auf TPP).

86 Vertraglich können Bank und Plattform aber die Schadenstragung untereinander im Innenverhältnis regeln.

87 Vgl. BGE 124 III 155 E. 3d, wo die Vertragsverletzung auf einer ungenügenden Aufklärung (also einer Unterlassung) gründete.

88 Siehe dazu *Reichart* (Fn. 56), 402 f.

89 Was in der Praxis wohl eher selten der Fall ist (anders aber z.B. BGer 9C_675/2011 vom 28.3.2012 E. 3.2).

90 BGE 146 III 387 E. 3.1; 146 III 121 E. 5. – Ausführlich dazu *Liégeois/Hirsch* (Fn. 62), 136 ff.

91 *Emmenegger/Thévenoz/Reber/Hirsch* (Fn. 59), 198.

92 Unklar das Bundesgericht in BGE 146 III 326 E. 4.2: «Lorsque les parties ont conclu une clause de transfert de risque, il n'y a pas de troisième étape comme c'est le cas lorsque le système légal s'applique […]. C'est dans le cadre de l'examen de la faute grave de la banque, qui est réservée (art. 100 al. 1 CO par analogie; cf. consid. 6 ci-dessous), que le juge doit ensuite examiner la faute concomitante du client comme facteur d'interruption du lien

4. Verantwortlichkeit der Bank für das Verhalten des TPP

4.1 Ausgangslage

In dieser Konstellation erleidet eine Kundin oder ein Kunde einen Vermögensschaden aufgrund eines sorgfaltswidrigen Verhaltens des TPP (z.B. eine nicht dem Risikoprofil angepasste Anlageempfehlung). Es stellt sich die Frage, unter welchen Umständen die Bank für diesen Schaden gegenüber ihrer Kundin bzw. ihrem Kunden aufgrund einer Sorgfaltspflichtverletzung (z.B. unterlassene Warn-, Informations- oder Aufklärungspflicht) schadenersatzpflichtig werden könnte (Art. 398 Abs. 2 i.V.m. Art. 97 Abs. 1 OR).

4.2 Sorgfalts- und Treuepflichten der Bank

Zwischen der Bank und den Kundinnen und Kunden besteht ein Bankvertrag, aus welchem auftragsrechtliche Sorgfalts- und Treuepflichten fliessen (Art. 398 OR).[93] Wie weit die Aufklärungs-, Informations- und Warnpflichten der Bank gehen, kann nicht allgemein festgelegt werden, sondern hängt von der Art des abgeschlossenen Vertrags und den Umständen des Einzelfalls ab. So spielen beim Anlageberatungsvertrag z.B. die Ausgestaltung des Beratungsverhältnisses, die Art des konkreten Anlagegeschäfts wie auch die Erfahrung und die Kenntnisse der Kundin/des Kunden eine Rolle.[94] Bei einem blossen Kontovertrag trifft die Bank die geringsten Aufklärungspflichten, da sie sich nur zu punktuellen Investitionsinstruktionen verpflichtet und nicht zu einer generellen Wahrung der Interessen der Kundin/des Kunden.[95]

Erteilt eine Kundin bzw. ein Kunde der Bank Weisungen zu kontorelevanten Verfügungen, trifft die Bank grundsätzlich keine Beratungspflicht, wenn die Kundin oder der Kunde zu erkennen gibt, dass er die Aufklärung weder benötigt noch wünscht.[96]

Eine Warnpflicht der Bank kann aber dennoch in Einzelfällen bestehen,[97] z.B. wenn die Bank bei pflichtgemässer Aufmerksamkeit erkennen muss, dass die Kundin oder der Kunde eine *bestimmte Gefahr* im Zusammenhang mit einer konkreten Anlage nicht erkannt hat oder wenn zwischen Bank und Kundin bzw. Kunde ein *besonderes Vertrauensverhältnis* beispielsweise aufgrund einer andauernden Geschäftsbeziehung besteht, aus welchem nach Treu und Glauben auch unaufgefordert Beratung oder Abmahnung erwartet werden darf.[98]

de causalité adéquate ou de réduction de l'indemnité qui lui est due.»; siehe dazu *Emmenegger/Thévenoz/Reber/Hirsch* (Fn. 59), 198, welche darauf hinweisen, dass nicht ersichtlich ist, auf welche Rechtsgrundlage sich das Bundesgericht stützt.

93 Zwischen Bank und Kundinnen und Kunden können bei Börsengeschäften verschiedene Vertragsbeziehungen im Vordergrund stehen: die blosse Konto-/Depotbeziehung (Execution-only), die Anlageberatung oder die eigentliche Vermögensverwaltung (vgl. BGer 4A_519/2020 vom 15.2.2019 E. 4.1). – Ähnlich auch BK-*Fellmann* (Fn. 44), Art. 398 N 430 und *Susan Emmenegger/Thirza Döbeli,* Kundenvertrauen in Banken, SZW 2017, 752 ff., 760 und 762.

94 BGer 4A_449/2018 vom 25.3.2019 E. 3.2. – Dazu BK-*Fellmann* (Fn. 44), Art. 398 N 434; *Emmenegger/Döbeli* (Fn. 93), 760 und 762 ff. sowie ausführlich *Sandro Abegglen,* Die Aufklärungspflichten in Dienstleistungsbeziehungen, insbesondere im Bankgeschäft, Diss. Universität Bern 1995, Bern 1995, 175 ff.

95 BGer 4A_54/2017 vom 29.1.2018 E. 5.1.4; 4C.385/2006 vom 2.4.2007 E. 2.1; 4A_369/2015 vom 25.4.2016 E. 2.3. – Vgl. *Emmenegger/Döbeli* (Fn. 93), 763 f.

96 BGE 133 III 97 E. 7.1.2; BGer 4A_449/2018 vom 25.3.2019 E. 3.1. – So kann sich z.B. ein Kunde auch nicht nach ausdrücklichem Einverständnis zur Verfolgung einer riskanten, spekulativen Anlagepolitik darauf berufen, sein Kundenprofil spräche für eine konservative, primär auf Erhaltung ausgerichtete Anlagepolitik, vgl. BGer 4A_140/2011 vom 27.6.2011 E. 2.1. Entsprechend könnte die Bank sich insofern exkulpieren, als der Kunde explizit – allenfalls sogar nach Abmahnung durch die Bank – die Zusammenarbeit mit einem TPP gewünscht hat, obwohl damit ein hohes Risiko verbunden war. – *Emmenegger/Döbeli* (Fn. 93), 763 f.

97 Wann eine solche Pflicht besteht, lässt sich jedoch nicht allgemein festlegen, sondern hängt von der Art des abgeschlossenen Vertrags und den Umständen des Einzelfalls ab (insbesondere Kenntnis und Erfahrung des Kunden), vgl. BGer 4A_54/2017 vom 29.1.2018 E. 5.1.3. – Sofern die Bank nur punktuell Geschäfte für den Kunden ausführt, besteht keine generelle Pflicht zur Interessenwahrung, und eine Aufklärung hat in der Regel nur auf Verlangen zu erfolgen, vgl. BGE 119 II 333 E. 5a und 131 III 377 E. 4.1.1. Ausserdem trifft die Bank keine Pflicht, sofern kein Informationsdefizit seitens der Kundinnen und Kunden vorliegt, vgl. BGer 4A_140/2011 vom 27.6.2011 E. 3.1 und 3.2, wo eine Aufklärungspflicht aufgrund der Sachkenntnis der Kunden abgelehnt wurde.

98 BGE 133 III 97 E. 7.1.2; BGer 4A_449/2018 vom 25.3.2019 E. 3.1; 4A_54/2017 vom 29.1.2018 E. 5.1.4; 4A_593/2015 vom 13.12.2016 E. 7.1.4. – Eine Pflicht wurde insbesondere bei erfahrungsgemäss hoch spekulativen und risikobehafteten Geschäften angenommen, wo der unerfahrene Kunde klar auf die Risken hinzuweisen und mit den daraus entstehenden Gefahren vertraut

4.3 Kooperationsmodelle

Für die Frage nach der Verantwortlichkeit der Bank für das sorgfaltswidrige Verhalten eines TPP bzw. Dienstleisters spielt es eine Rolle, welches Kooperationsmodell vorliegt. So ist im Hinblick auf das Ausmass der Sorgfalts- und Treuepflichten (Warn-, Informations-, Aufklärungspflichten) zum einen relevant, wie eng sich die Beziehung zwischen Bank und TTP bzw. Dienstleister gestaltet,[99] und zum anderen ist entscheidend, wie das Vertragsverhältnis zwischen Bank und Kundinnen und Kunden sich präsentiert; aber auch das Verhältnis zwischen Kundinnen und Kunden und TPP bzw. Dienstleister.

Wenig Unklarheiten bestehen beim *«Outsourcing»;* dort trägt die Bank die Verantwortung für den Dienstleister nach den Regeln der Hilfspersonenhaftung (Ziff. III.1.1).[100]

Etwas weniger klar ist die Ausgangslage beim *«gemeinsamen Angebot»* und im *«Plattformmodell».* Dort haften die beiden Parteien – Bank und TPP – den Kundinnen und Kunden grundsätzlich für die gemeinsam geschuldete Leistung («Open Banking-Dienstleistung») solidarisch (Ziff. III.1.2).

Trifft nur den unsorgfältigen TPP ein Verschulden, so haftet gestützt auf den Vertrag über die gemeinsame Leistung grundsätzlich auch nur er den Kundinnen und Kunden (bei gegebenen Voraussetzungen) für den erlittenen Schaden. Die Bank haftet demgegenüber in diesen Kooperationsmodellen grundsätzlich nicht, wenn nur den TPP ein Verschulden trifft (Ziff. III.1.2).

Eine solche Haftung der Bank könnte sich aber allenfalls aus der Verletzung einer Sorgfaltspflicht ergeben, welche in erster Linie aus dem unterliegenden Bankvertrag, aber auch aus dem Vertrag über die «Open Banking-Dienstleistung» fliessen kann. Dabei spielen unterschiedliche Faktoren eine Rolle. So z.B. die konkrete *Art der Vertragsbeziehung* zwischen Bank und Kundinnen und Kunden. Je mehr die Bank vertraglich eine Beratung oder Unterstützung zugesichert hat (z.B. Anlageberatung), je intensiver die Bankbeziehung ist, je grösser das Wissen der Bank über die Kundin oder den Kunden (z.B. Risikoprofil), desto eher dürfen die Kundinnen und Kunden darauf vertrauen, dass die Bank ganz allgemein ihre Interessen wahrt. Ebenfalls relevant ist die Art und Weise, wie die Bank die gemeinsame Dienstleistung mit dem TPP den Kundinnen und Kunden konkret *empfiehlt.* Je vorbehaltsloser die Bank die «Open Banking-Dienstleistung» den Kundinnen und Kunden präsentiert, desto mehr erweckt die Bank bei ihnen das Vertrauen, dass diese vom TPP den gleichen (Sicherheits-)Standard erwarten können wie von ihrer Bank und desto eher könnte eine Sorgfaltspflicht der Bank begründet werden, den TPP bei der Auswahl zu prüfen und zu überwachen.[101]

Wiederum klarer ist die Ausgangslage im Kooperationsmodell der *«einseitigen Aufforderung».* In diesem Modell treffen die Bank die geringsten Sorgfaltspflichten. In dieser Konstellation kommt dem TTP eine ähnliche Funktion zu wie z.B. einem privaten Vermögensberater der Kundinnen und Kunden, weshalb die Bank keine Pflicht trifft, den TPP auszuwählen oder diesen zu überwachen.[102] Allenfalls könnte es aus der Sicht der Bank sinnvoll sein, die Kundinnen und Kunden bei Freigabe der Schnittstelle bzw. API darüber aufzuklären, dass sie den TPP nicht geprüft habe, ihn auch nicht überwachen wird und die Inanspruchnahme der Dienstleistung auf Gefahr der Kundinnen und Kunden geschehe. Nur in seltenen Fällen – z.B. wenn die Bank im Zusammenhang mit einem bestimmten TPP eine konkrete Gefahr kennt, indem sie über negative Informationen zu diesem verfügt, oder wenn sie ein besonderes Vertrauensverhältnis zur Kundin oder zum Kunden hat – könnte sie eine Pflicht zur Beratung bzw. Abmahnung treffen.[103] Sollte die Bank aufgrund einer Sorgfaltspflichtverletzung in einem solchen Fall ausnahmsweise eine Haftung treffen, drängt sich in dieser Ausgangslage die

zu machen ist, vgl. BGE 124 III 155 E. 3a. – Dazu auch *Emmenegger/Döbeli* (Fn. 93), 763.

99 SBVg (Fn. 7), 24.

100 FINMA-Outsourcing (Fn. 9), Rz. 23.

101 Vgl. dazu BGE 133 III 97 E. 7.2, wonach es keiner formellen Grundlage bedarf, «wenn sich wegen einer andauernden Geschäftsbeziehung zwischen der Bank und dem Kunden ein besonderes Vertrauensverhältnis entwickelt hat, aus welchem der Kunde nach Treu und Glauben auch unaufgefordert Beratung und Abmahnung erwarten darf.» – Vgl. *Emmenegger/Döbeli* (Fn. 93), 754, die erwähnen, dass «die Kundinnen und Kunden darauf vertrauen, dass die Bank ihre Aktivitäten an den Kundeninteressen orientiert, dass sie also diejenigen Produkte empfiehlt oder ins Kundenportfolio legt, die für den Kunden die besten sind …», was auch auf TPPs zutreffen könnte.

102 Vgl. BGer 4A_449/2018 vom 25.3.2019 E. 3.1 sowie BGE 119 II 333 E. 5a; 133 III 97 E. 7.1.1 und 7.1.2.

103 Vgl. z.B. BGE 133 III 97 E. 7.1.2.

Prüfung einer Reduktion des Schadenersatzes aufgrund von Selbstverschulden der Kundinnen und Kunden auf (Art. 44 Abs. 1 i.V.m. Art. 99 Abs. 3 OR).

5. Fazit vertragsrechtliche Haftung

Wer für den Vermögensschaden infolge eines Legitimationsmangels (z.B. «Man-in-the-Middle»-Attacke) vertragsrechtlich verantwortlich ist und ob die Bank ihren Kundinnen und Kunden aufgrund eines sorgfaltswidrigen Verhaltens des TPP schadenersatzpflichtig wird, hängt stark vom vorliegenden Kooperationsmodell ab. Während die Bank im Falle eines *«Outsourcings»* die gesamte Verantwortung gegenüber den Kundinnen und Kunden trägt, nimmt diese Verantwortung bei *«gemeinsamen Angeboten»* und in den *«Plattformmodellen»* bereits ab. Im Falle von *«einseitigen Aufforderungen»* der Kundinnen und Kunden an ihre Bank wird diese schliesslich nur in Ausnahmefällen für Vermögensschäden einstehen müssen.

IV. Datenschutzrechtliche Ansprüche und Bussenrisiko

1. Fragestellung

Datendiebstähle haben in den vergangenen Jahren stark zugenommen.[104] Darunter fallen unter anderem die 2014 erfolgten Hackerangriffe auf die amerikanische Grossbank J.P.Morgan, bei welchem Daten von 76 Millionen Haushalten und 7 Millionen Unternehmen erbeutet werden konnten,[105] oder jener auf die E-Banking-Konten der Kundinnen und Kunden von 12 Schweizer Banken.[106] Der im Februar 2015 bei einer Krankenkasse erfolgte Datendiebstahl von über 80 Millionen Versicherten zeigt, dass auch Versicherungen im Fokus von Hackern stehen.[107]

Open Banking, dessen Kerninhalt der Austausch und die Übermittlung von Kundendaten zwischen zwei oder mehreren Parteien ist, erhöht zumindest theoretisch die Wahrscheinlichkeit von Datenpannen («data breaches») wie z.B. Datendiebstählen. Im Folgenden wird für die vorgestellten Kooperationsformen untersucht, wer für die Sicherstellung des Datenschutzes[108] verantwortlich ist. Gestützt darauf ist die Frage zu beantworten, *a)* gegen wen sich allfällige datenschutzrechtliche Ansprüche aus einem Datenschutzverstoss richten und *b)* wer einem Bussenrisiko ausgesetzt ist. Nicht behandelt wird die Frage, welche Massnahmen zur Gewährleistung der Datensicherheit für eine bestimmte Datenbearbeitung zu treffen sind, weil dies nur einzelfallweise aufgrund der konkreten Umstände beantwortet werden kann.

2. Rechtliche Grundlagen

Die nachstehenden Ausführungen fokussieren sich auf eine Übersicht der *Massnahmen zur Sicherstellung der Datensicherheit,* welchen im Rahmen von Open Banking aufgrund des Daten*austauschs* zwischen Bank und TPP besondere Bedeutung zukommt. Auf die weiteren datenschutzrechtlichen Vorschriften wie beispielsweise die Bearbeitungsgrundsätze, die Informationspflichten oder die Betroffenenrechte wird an dieser Stelle nicht näher eingegangen.

104 Siehe die Übersicht nur einiger grosser Datendiebstahlfälle, *René Schmid,* Datendiebstähle in den vergangenen Jahren, abrufbar unter: <*https://www.fhnw.ch/plattformen/iwi/2019/04/15/datendiebstaehle-in-den-vergangenen-jahren-2/*> (zuletzt besucht: 13.1.2022). – Ein neueres Beispiel ist auch der Hackerangriff auf den Vergleichsdienst Comparis (dazu Luzerner Zeitung vom 30. Juli 2021, Nach Hackerangriff: Comparis knickt ein und zahlt Lösegeld, abrufbar unter: <*https://www.luzernerzeitung.ch/wirtschaft/cyberkriminalitaet-nach-hackerangriff-comparis-knickt-ein-und-zahlt-loesegeld-ld.2168629*> [zuletzt besucht: 13.01.2022]).

105 Vgl. NZZ vom 4. Oktober 2014, Kundendaten sind eine leichte Beute, abrufbar unter: <*https://www.nzz.ch/wirtschaft/kundendaten-sind-eine-leichte-beute-1.18396277*> (zuletzt besucht: 13.01.2022).

106 Vgl. Tagesanzeiger vom 22. Juli 2014, Hackerangriff auf Schweizer Banken, abrufbar unter: <*https://www.tagesanzeiger.ch/wirtschaft/unternehmen-und-konjunktur/hackerangriff-auf-schweizer-banken/story/20194915*> (zuletzt besucht: 13.1.2022).

107 Vgl. Frankfurter Allgemeine vom 5. Februar 2015, Hackerangriff auf Amerikas zweitgrössten Krankenversicherer, abrufbar unter: <*https://www.faz.net/aktuell/wirtschaft/unternehmen/hackerangriff-auf-us-krankenversicherer-anthem-13410690.html*> (zuletzt besucht: 13.1.2022).

108 Kundeninformationen unterstehen als Personendaten dem revDSG, vgl. dazu Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017 6941 ff., 7019.

2.1 Massnahmen zur Sicherstellung des Datenschutzes

Der in Art. 8 Abs. 1 revDSG[109] festgehaltene risikobasierte Ansatz[110] verpflichtet sowohl den Verantwortlichen als auch den Auftragsbearbeiter, geeignete technische[111] und organisatorische[112] Massnahmen («TOMs») zu treffen, um *Verletzungen der Datensicherheit*[113] zu vermeiden.[114] Die Mindestanforderungen an die Datensicherheit werden in der Verordnung (VDSG)[115] spezifiziert. Überträgt ein Verantwortlicher eine Datenbearbeitung an einen Auftragsbearbeiter, so hat er sich gemäss Art. 9 Abs. 2 revDSG zu vergewissern, dass der betreffende Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten. Im Falle einer Verletzung der Datensicherheit hat der Verantwortliche den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) sowie – unter gewissen Voraussetzungen – die betroffenen Personen zu informieren (Art. 24 revDSG).

Vorkehrungen zur Verhinderung *anderer Datenschutzverletzungen* sind in Art. 7 revDSG enthalten. Demnach ist der Verantwortliche verpflichtet, die Datenbearbeitung technisch und organisatorisch so auszugestalten, dass die Datenschutzvorschriften, insbesondere die Bearbeitungsgrundsätze nach Art. 6 revDSG, eingehalten werden («Privacy by Design»; Abs. 1 und 2). Zudem muss er mittels geeigneter Voreinstellungen sicherstellen, dass die Bearbeitung der Personendaten auf das für den Verwendungszweck nötige Mindestmass beschränkt ist («Privacy by Default»; Abs. 3). Dem Auftragsbearbeiter werden keine entsprechenden Pflichten auferlegt.

Die Frage, wer welche Massnahmen zur Sicherstellung des Datenschutzes zu treffen hat, hängt somit davon ab, in welcher «Rolle» (als Verantwortlicher[116] oder Auftragsbearbeiter[117]) jemand Personendaten bearbeitet. Entsprechend gilt es vorab zu klären, ob es sich bei den in eine Datenbearbeitung involvierten Personen um (eigenständige oder gemeinsam) Verantwortliche oder um Auftragsbearbeiter handelt.

2.2 Folgen eines Datenschutzverstosses

Die Verletzung der Datensicherheit nach Art. 8 revDSG ist gemäss Art. 30 Abs. 2 lit. a revDSG eine Persönlichkeitsverletzung. Daraus erwachsende zivilrechtliche Rechtsansprüche können gemäss Art. 32 Abs. 2 revDSG i.V.m. Art. 28 ZGB gegenüber *jeder an der Verletzung mitwirkenden Person* geltend gemacht werden.[118] Im Falle einer gemeinsamen Datenbearbeitung kann das ein (Mit-)Verantwortlicher sein, im Falle einer Auftragsbearbeitung auch der Auftragsbearbeiter. Aus haftpflichtrechtlicher Perspektive haften die involvierten Parteien dem Geschädigten nach Massgabe von Art. 50 OR solidarisch.[119] Bei der Auftragsbearbeitung dürfte seitens des Verantwortlichen regelmässig auch die Geschäftsherrenhaftung nach Art. 55 OR greifen.[120] Besteht zwischen dem Verantwortlichen und der betroffenen Person ein Vertrag, ist sodann eine Hilfspersonenhaftung nach Art. 101 OR möglich.[121]

Im Falle einer (eventual-)vorsätzlichen Verletzung der Mindestanforderungen an die Datensicherheit (Art. 8 revDSG) wird der *verantwortliche Mitarbeitende* des Verantwortlichen bzw. Auftragsbearbeiters auf Antrag mit Busse bis zu CHF 250 000 bestraft (Art. 61 lit. c revDSG). Gleiches gilt, wenn der Verantwortliche seine Pflichten bei der Übertragung einer Datenbearbeitung an einen Auftragsbearbeiter nach Art. 9 revDSG verletzt, insbesondere indem er

109 Im Folgenden wird auf die Bestimmungen des totalrevidierten Datenschutzgesetzes (revDSG) fokussiert, welches bereits verabschiedet ist und voraussichtlich Anfang 2023 in Kraft gesetzt werden wird; Schlussabstimmungstext unter: <*https://www.fedlex.admin.ch/eli/fga/2020/1998/de*> (zuletzt besucht: 13.1.2022).

110 Dazu Botschaft DSG 2017 (Fn. 108), 7031: «Je grösser das Risiko einer Verletzung der Datensicherheit, umso höher sind die Anforderungen an die zu treffenden Massnahmen».

111 Dazu gehören z.B. Anonymisierungen, Pseudonymisierungen und Verschlüsselungen, vgl. *Rolf H. Weber/Simon Henseler,* Daten-Governance und Cloud Banking im neuen Datenschutzumfeld, SZW 2020, 604 ff., 614.

112 Hierzu gehören beispielsweise vertragliche Abreden, interne Weisungen und definierte Prozesse, vgl. *Weber/Henseler* (Fn. 111), 614.

113 Zur Definition: Art. 5 Bst. h revDSG.

114 Siehe hierzu auch Botschaft DSG 2017 (Fn. 108), 7031.

115 Die revidierte Verordnung zum Datenschutzgesetz liegt derzeit noch nicht final vor.

116 Sog. «Controller».

117 Sog. «Processor».

118 Vgl. *David Rosenthal,* Controller oder Processor: Die datenschutzrechtliche Gretchenfrage, Jusletter vom 17. Juni 2019, Rz. 67 Fn. 77.

119 Vgl. *Rosenthal* (Fn. 118), Rz. 67 Fn. 77.

120 *David Rosenthal,* Das neue Datenschutzgesetz, Jusletter 16. November 2020, Rz. 61.

121 *Rosenthal* (Fn. 120), Rz. 61.

den Auftragsbearbeiter nicht zur weisungsgebundenen Bearbeitung verpflichtet oder sich nicht vergewissert, dass dieser in der Lage ist, die Datensicherheit zu gewährleisten (Art. 61 lit. b revDSG). Die Regelung von Art. 7 revDSG («Privacy by Design» und «Privacy by Default») ist nicht sanktionsbedroht.

2.3 Verantwortlicher und Auftragsbearbeiter

Die Abgrenzung zwischen Verantwortlichem und Auftragsbearbeiter ist in der Praxis zuweilen schwierig.[122] Dem funktionellen Konzept[123] folgend, ist bei der Rollenzuteilung – jeweils in Bezug auf eine konkrete Datenbearbeitung – massgebend, wer über den *Zweck* («wozu» bzw. «weshalb») und die wesentlichen *Mittel* («wie» bzw. «auf welche Art») entscheidet.[124] Die Zuteilung entzieht sich damit der Parteidisposition.[125]

Gemäss Art. 5 lit. j revDSG gilt derjenige, der allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung entscheidet als Verantwortlicher.[126] Werden Daten im Auftrag und nach Weisung eines Verantwortlichen bearbeitet, liegt hingegen eine Auftragsbearbeitung vor (Art. 5 lit. k revDSG).[127]

Auch wenn es sich um einen externen Dienstleister handelt, gilt der Auftragsbearbeiter datenschutzrechtlich nicht als Dritter.[128] Seine Datenbearbeitung ist vielmehr dem Verantwortlichen zuzurechnen.[129] So hält Art. 9 Abs. 1 lit. a revDSG denn auch fest, dass der Auftragsbearbeiter die Daten nur so bearbeiten darf, wie es der Verantwortliche selbst tun dürfte. Entsprechend hat der Verantwortliche sicherzustellen, dass seine Weisungen kein anwendbares (Datenschutz-)Recht verletzen. Weiter sieht Art. 9 Abs. 2 revDSG vor, dass sich der Verantwortliche insbesondere vergewissern müsse, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten.[130] Den Auftragsbearbeiter trifft von Gesetzes wegen eine geringere datenschutzrechtliche Verantwortung (vgl. insbesondere Art. 1 ff. und Art. 25 ff. revDSG, die lediglich den Verantwortlichen adressieren).[131] Gleichwohl existieren einige – wichtige – gesetzliche Pflichten, die (auch) den Auftragsbearbeiter adressieren. Dazu gehört insbesondere die strafbewehrte Pflicht zur Gewährleistung der Datensicherheit (vgl. Ziff. IV.2.1).[132]

Die Übertragung einer Bearbeitung von Personendaten an einen Auftragsbearbeiter hat gemäss Art. 9 revDSG – schriftlich oder mündlich[133] – mittels Auftragsbearbeitungsvertrags («ADV») zu erfolgen. Die Personendaten dürfen vom Auftragsbearbeiter nur so bearbeitet werden, wie es der Verantwortliche darf, und die Übertragung der Bearbeitung an einen Dritten bedarf einer vorgängigen Genehmigung des Verantwortlichen. Bei der Ausgestaltung des ADV ist eine Orientierung an der Regelung der DSGVO[134] hilfreich, die – anders als das revDSG – einen Mindestinhalt vorschreibt. Die Parteien sind frei, weitere Vereinbarungen (z.B. Haftungsregelung, Kostentragung) zu treffen.

122 *Rosenthal* (Fn. 118), *passim*.

123 Dazu ausführlich Artikel-29-Datenschutzgruppe, Stellungnahme 1 | 2010 zu den Begriffen «für die Verarbeitung Verantwortlicher» und «Auftragsbearbeiter» vom 16. Februar 2010 (WP 169), 12.

124 Vertieft *David Rosenthal/Barbara Epprecht,* Banken und ihre datenschutzrechtliche Verantwortlichkeit im Verkehr mit ihren Dienstleistern, in: Susan Emmenegger (Hrsg.), Banken und Datenschutz, Basel 2019, 127 ff., 136 ff. und 139 ff.

125 Vgl. *Rosenthal/Epprecht* (Fn. 124), 135; *Rosenthal* (Fn. 118), Rz. 25.

126 *Rosenthal/Epprecht* (Fn. 124), 130; *Rosenthal* (Fn. 118), Rz. 11.

127 *Roth* (Fn. 3), 682.

128 *Rosenthal* (Fn. 118), Rz. 4; *Rosenthal/Epprecht* (Fn. 124), 133 f.

129 *Rosenthal* (Fn. 118), Rz. 4; *Rosenthal/Epprecht* (Fn. 124), 133 f.

130 *Roth* (Fn. 3), 681 f.

131 Vgl. *Rosenthal/Epprecht* (Fn. 124), 131.

132 Siehe für eine ausführliche Aufzählung der Pflichten des Verantwortlichen und des Auftragsbearbeiters, *Rosenthal/Epprecht* (Fn. 124), 131 ff.

133 Nach Art. 28 Abs. 9 DSGVO ist der ADV zwingend schriftlich abzuschliessen; siehe auch zur Ausgangslage vor dem revDSG *Roland Mathys,* IT-Outsourcing-Vertrag, in: WEKA Verlag AG (Hrsg.), Informatikrecht in der Praxis, Zürich 2008, Kapitel 5/6.3.3, 12 f., wonach es auch schon damals der Praxis entsprach, bei der Auslagerung gewisser Geschäftstätigkeiten allfällige datenschutzrechtliche Fragen vertraglich zu regeln.

134 Art. 28 Abs. 3 DSGVO, insbesondere folgende Punkte gilt es zu beachten: Gegenstand, Dauer, Art und Zweck der Verarbeitung, Art der personenbezogenen Daten, Kategorien betroffener Personen sowie Pflichten und Rechte des Verantwortlichen.

2.4 Eigenständige oder gemeinsame Verantwortliche

Als Verantwortlicher gilt, wer *allein oder zusammen mit anderen* über den Zweck und die Mittel der Bearbeitung entscheidet (Art. 5 lit. j revDSG). Wer allein entscheidet, gilt als *eigenständiger* Verantwortlicher, wer dies gemeinsam mit anderen tut, als *gemeinsam* Verantwortlicher, wobei dafür bereits ein arbeitsteiliges Zusammenwirken ausreicht.[135] Massgebend ist, dass es um dieselbe Bearbeitung geht, d.h. zwischen den Bearbeitungen der Verantwortlichen ein «untrennbares Band» besteht.[136]

Die Beurteilung, ob ein gemeinsames Bestimmen des Zwecks bzw. der Mittel und damit eine gemeinsame Verantwortlichkeit vorliegt, hat aufgrund der konkreten Umstände im Einzelfall zu erfolgen. Der EuGH setzt dabei die Schwelle tief an, um einen möglichst umfassenden Schutz der Betroffenen zu gewährleisten.[137] Es genügt demnach die blosse *Einflussnahme* auf die Datenbearbeitung; ein direkter Datenzugang und eine unmittelbare Mitbestimmung bei der Bearbeitung sind nicht erforderlich.[138]

Das revDSG enthält – im Gegensatz zur DSGVO[139] – keine Pflicht der *gemeinsam* Verantwortlichen, eine Vereinbarung über die Bearbeitung abzuschliessen. Gleichwohl kann eine solche Vereinbarung sinnvoll sein, einerseits, damit die Parteien vom gleichen Rollenverständnis («gemeinsame Verantwortlichkeit») ausgehen, und andererseits, um die gegenseitige Einhaltung des Datenschutzes sicherzustellen. Letzteres ist insbesondere aufgrund der solidarischen Haftung relevant (vgl. Ziff. IV.2.2).

Eigenständige Verantwortliche, die gegenseitig Personendaten austauschen, haben weder unter revDSG noch unter DSGVO die Pflicht, eine Vereinbarung abzuschliessen. Gleichwohl empfiehlt sich unter Umständen auch in dieser Konstellation eine vertragliche Regelung, um datenschutzrechtlich relevante Aspekte wie beispielsweise die Zweckbindung der jeweiligen Bearbeitung, die Vertraulichkeit der erhaltenen Personendaten oder auch die Gewährleistung der Datensicherheit sicherzustellen.[140]

3. Einordnung der Kooperationsformen

3.1 «Outsourcing»

Bei der Auslagerung einer Geschäftstätigkeit an einen Dritten erfolgt regelmässig auch eine Übertragung der Datenbearbeitung. Dabei fällt ausschliesslich die (auslagernde) Bank den Entscheid über den Zweck und die Mittel der Bearbeitung und qualifiziert somit als (eigenständige) Verantwortliche nach Art. 5 lit. j revDSG.[141] Der Dienstleister, an den die Geschäftstätigkeit ausgelagert wird, bearbeitet die Daten in der Regel ausschliesslich im Auftrag und nach Weisung der Bank und qualifiziert somit als Auftragsbearbeiter nach Art. 5 lit. k revDSG.[142] Sofern und soweit der Dienstleister keine eigenmotivierten, nicht weisungsgemässen Bearbeitungen vornimmt,[143] bleibt die datenschutzrechtliche Verantwortlichkeit bei der Bank.[144]

Als Verantwortlicher hat die Bank insbesondere die Massnahmen zur Sicherstellung des Datenschutzes nach Art. 7 und Art. 8 revDSG zu treffen. Vor der Übertragung der Datenbearbeitung an den Dienstleister muss sie sich zudem vergewissern, dass dieser in der Lage ist, die Datensicherheit zu gewährleisten (vgl. Ziff. IV.2.1).

Falls die Bank gegen ihre Pflicht zur Sicherstellung der Datensicherheit verstösst und der betroffenen Person (Bankkundin bzw. Bankkunde) ein datenschutzrechtlicher Anspruch zukommt, ist dieser gegenüber der Bank geltend zu machen. Falls hingegen der Dienstleister eine Verletzung der Datensicherheit begeht, stellt sich die Frage, ob die Bank an dieser Persönlichkeitsverletzung «mitgewirkt» hat. Ist dies zu bejahen, z.B. weil sie den Dienstleister nicht ordnungsgemäss geprüft hat, kann die Kundin bzw. der Kunde ihre bzw. seine datenschutzrechtlichen Ansprüche sowohl gegenüber dem Dienstleister als auch gegenüber der Bank geltend machen.

135 *Rosenthal* (Fn. 120), Rz. 13.
136 *Rosenthal* (Fn. 120), Rz. 13.
137 Urteil des EuGH vom 5.6.2018 (C-210/16) i.S. Wirtschaftsakademie Schleswig-Holstein, EU:C:2018:388, N 36 und 42.
138 Vgl. Urteil des EuGH vom 10.7.2018 (C-25/17) i.S. Zeugen Jehovas, EU:C:2018:551, N 66 ff. und *Rosenthal/Epprecht* (Fn. 124), 142 f.
139 Vgl. Art. 26 DSGVO.
140 *Rosenthal* (Fn. 118), Rz. 114.
141 Vgl. *Rosenthal/Epprecht* (Fn. 124), 130 f.
142 Vgl. *Rosenthal/Epprecht* (Fn. 124), 130.
143 Diesfalls würde er ebenfalls Verantwortlicher, vgl. *Roth* (Fn. 3), 682 und *Rosenthal/Epprecht* (Fn. 124), 130.
144 Vgl. *Rosenthal/Epprecht* (Fn. 124), 130; *Mathys* (Fn. 133), 12 m.w.H.

Dem für die Datenpanne verantwortlichen Mitarbeitenden droht zudem eine Busse, wenn er die Mindestanforderungen an die Datensicherheit (eventual-)vorsätzlich nicht eingehalten hat, wobei es keine Rolle spielt, ob es sich um einen Mitarbeitenden der Bank oder des Dienstleisters handelt. Zudem droht dem verantwortlichen Mitarbeitenden der Bank eine Busse, wenn er sich (eventual-)vorsätzlich nicht vergewissert hat, dass der Dienstleister in der Lage ist, die Datensicherheit zu gewährleisten. Eine Sanktionierung setzt in jedem Fall einen entsprechenden Strafantrag voraus (vgl. Ziff. IV.2.2).

3.2 «Gemeinsame Angebote»

Anders als beim *«Outsourcing»* tritt der TPP bei einem gemeinsamen Angebot im Aussenauftritt neben die Bank, was bei den Kundinnen und Kunden den Eindruck entstehen lassen kann, einer Mehrzahl von Verantwortlichen gegenüberzustehen. Dies ist mit Blick auf die datenschutzrechtliche Rollenzuteilung ein Indiz dafür, dass ein TPP nicht als Auftragsbearbeiter, sondern als Verantwortlicher zu qualifizieren ist.[145] Anders als der Dienstleister im *«Outsourcing»* bearbeitet der TPP die von der Bank erhaltenen Personendaten nicht dazu, eine ihm übertragene Funktion für die Bank auszuüben.

Die den Kundinnen und Kunden *gemeinsam* vertraglich versprochene Leistung kann beim gemeinsamen Angebot sehr unterschiedlich ausgestaltet sein. So kann sie auf die blosse *Abwicklung* der «Open Banking-Dienstleistung» über die Schnittstelle bzw. API beschränkt sein. Je nach Intensität der Zusammenarbeit kann aber auch der *Gegenstand* der «Open Banking-Dienstleistung» gemeinsam von TPP und Bank geschuldet sein (vgl. Ziff. III.1.2).

Für jene Datenbearbeitungen, für welche die Bank und der TPP den Zweck und die Mittel gemeinsam festlegen – z.B. den Transfer spezifizierter Daten über eine spezifisch ausgestaltete Schnittstelle bzw. API – liegt eine gemeinsame Verantwortlichkeit vor.[146] Für die übrigen Datenbearbeitungen sind TPP und Bank je (eigenständig) verantwortlich.

Führt ein Datenschutzverstoss im Falle der gemeinsamen Verantwortlichkeit zu einer Persönlichkeitsverletzung, so können aufgrund der beidseitigen Mitwirkung sowohl die Bank als auch der TPP ins Recht gefasst werden – sie haften solidarisch (vgl. Ziff. IV.2.2). Vorbehalten bleibt die Klagemöglichkeit gestützt auf Vertragsrecht.

Dies ändert sich allerdings dort, wo TPP und Bank eigenständig verantwortlich sind. Dort sind je nachdem, ob die Verletzung der Datensicherheit durch die Bank oder den TPP erfolgt, daraus resultierende datenschutzrechtliche Ansprüche gegen die Bank bzw. den TPP zu richten. In diesem Fall ist eine solidarische Haftung der Parteien ausgeschlossen, weil diese gegenseitig nicht an der Sicherstellung der Datensicherheit beteiligt sind und damit auch nicht an der Verletzung «mitwirken» können.

Das Bussenrisiko bei einer Verletzung der Mindestanforderungen an die Datensicherheit trifft die jeweils verantwortlichen Mitarbeitenden der Parteien (vgl. Ziff. IV.2.2).

3.3 «Plattform»

Zunächst gilt es auch in diesem Kooperationsmodell, die datenschutzrechtliche Rollenzuteilung vorzunehmen, d.h. zu analysieren, welche Partei(en) den Zweck und die Mittel der jeweiligen Datenbearbeitung festlegt. Dabei ist insbesondere die Frage zu klären, ob auch die Plattformbetreiberin einen entscheidenden Einfluss hat.

Beschränkt sich die Tätigkeit der Plattform bezüglich einer bestimmten Datenbearbeitung auf den (weisungsgebundenen) Informationsaustausch zwischen TPP und Bank, also auf eine reine «Datenübermittlungstätigkeit», ist tendenziell von einer Auftragsbearbeitung auszugehen. Indizien für eine Qualifikation der Plattform als Auftragsbearbeiterin können eine weisungsgebundene Ausgestaltung und Bereitstellung von Schnittstellen bzw. API, die Entscheidungsfreiheit der Plattformnutzer bezüglich der Kooperation mit anderen Plattformnutzern[147] oder die Zusicherung eines sicheren und unveränderten Übermittlungsvorgangs[148] sein.[149]

145 Nach *Rosenthal/Epprecht* (Fn. 124), 130, ist dies mitentscheidend, ob ein Verantwortlicher vorliegt.

146 Vgl. die Unterscheidung in diesem Punkt für das Modell der *«einseitigen Aufforderung»*.

147 Insbesondere auch der Entscheid, ob und in welchem Umfang die Plattformnutzer Zugriff auf die jeweiligen Informationen gewähren, vgl. als Beispiel Teilnahmebedingungen (Fn. 31), Rz. 39.

148 So beispielsweise Teilnahmebedingungen (Fn. 31), Rz. 16b und 19.

149 Ähnlich auch *Roth* (Fn. 3), 683 f.

Bestimmt hingegen die Plattformbetreiberin über wesentliche Mittel einer Datenbearbeitung – beispielsweise die Zulassungsprüfung – kann sie für diese Datenbearbeitung (auch) als Verantwortliche qualifizieren. Dasselbe würde beispielsweise auch gelten, wenn sich die Plattform vorbehält, die von der Bank und/oder dem TPP erhaltenen Personendaten für weitere («eigene») Zwecke, z.B. Marketing, zu verwenden.

Hinweise auf die Zwecke der Datenbearbeitungen sind regelmässig der Datenschutzerklärung oder anderen Datenschutzhinweisen der Plattform sowie den Verträgen zwischen den Parteien zu entnehmen. Allerdings ist die datenschutzrechtliche Qualifikation, wie erwähnt, der Parteidisposition entzogen (vgl. Ziff. IV.2.3).

Die Beurteilung der datenschutzrechtlichen Verantwortlichkeit für eine Verletzung der Datensicherheit ist dementsprechend je nach konkreter Ausgestaltung der Plattform und auch für jede einzelne Datenbearbeitung separat vorzunehmen. Denkbar sind in einem *«Plattformmodell»* alle Varianten, also Auftragsbearbeitung[150] sowie eigenständige und gemeinsame Verantwortlichkeit[151].

Das Bussenrisiko bei einer Verletzung der Mindestanforderungen an die Datensicherheit trifft die jeweils verantwortlichen Mitarbeitenden der Parteien (vgl. Ziff. IV.2.2).

3.4 «Einseitige Aufforderung»

Die *«einseitige Aufforderung»* zeichnet sich dadurch aus, dass die Kundin bzw. der Kunde die Bank beauftragt, ihre/seine Kontoinformationen an einen Dritten zu übermitteln. Obwohl die Bank die durch die Kundin bzw. den Kunden gewünschten Informationen dem TPP übermittelt und somit im Auftrag ihrer Kundin oder ihres Kunden handelt, bleibt sie Verantwortliche, denn sie veranlasst und steuert die Datenbearbeitung selbst, womit sie eigenständig die Zwecke und Mittel der Datenbearbeitung festlegt, ohne dass ein arbeitsteiliges Zusammenwirken mit ihren Kundinnen und Kunden vorliegt.[152]

Der TPP hat in Bezug auf die Daten regelmässig keine Weisungen der Bank zu befolgen, und seine Datenbearbeitung erfolgt, um die «eigene» Finanzdienstleistung zu erbringen. Der TPP definiert das erwartete Ergebnis oder leitet die geplante Aktion[153] und legt damit den Zweck und die wesentlichen Mittel selbständig fest.[154]

Im Falle der *«einseitigen Aufforderung»* liegt – anders als beim *«gemeinsamen Angebot»* – auch in Bezug auf die Datenbearbeitungen an der Schnittstelle bzw. API keine gemeinsame Verantwortlichkeit vor. So kann die Bank die Ausgestaltung der Schnittstellen bzw. APIs in ihrem System selbst gestalten und legt damit die Mittel der Datenbearbeitung selbständig fest. Bank und TPP haben folglich eigene Sphären, für die sie verantwortlich sind, auch wenn diese sich «berühren»,[155] weshalb sie als eigenständige Verantwortliche zu qualifizieren sind.[156]

Werden TPP und Bank als eigenständige Verantwortliche qualifiziert, sind je nachdem, durch wen die Verletzung der Datensicherheit erfolgt, daraus resultierende datenschutzrechtliche Ansprüche gegen die Bank bzw. den TPP zu richten. In diesem Fall ist eine solidarische Haftung der Parteien ausgeschlossen, weil diese gegenseitig nicht an der Sicherstellung der Datensicherheit beteiligt sind und damit auch nicht an der Verletzung «mitwirken» können.

Das Bussenrisiko bei einer Verletzung der Mindestanforderungen an die Datensicherheit trifft die jeweils verantwortlichen Mitarbeitenden der Parteien (vgl. Ziff. IV.2.2).

4. Fazit Datenschutz

Open Banking, dessen Kerninhalt der Austausch und die Übermittlung von Kundendaten zwischen zwei oder mehreren Parteien ist, erhöht zumindest theoretisch die Wahrscheinlichkeit von Datenpannen («data breaches») wie z.B. Datendiebstählen.

Wer für welche (strafbewehrten) Pflichten zur Sicherstellung der Datensicherheit zuständig ist, hängt insbesondere davon ab, wer im Sinne der Datenschutzgesetzgebung als «Verantwortliche/r» und wer ggf. als «Auftragsbearbeiter/in» qualifiziert. Das diesbezügliche Bussenrisiko tragen jedoch nicht die Unternehmen, sondern die jeweilige Mitarbeiterin

150 Vgl. zu den Folgen Ziff. IV.3.1.
151 Vgl. je zu den Folgen Ziff. IV.3.2.
152 Vgl. *Rosenthal/Epprecht* (Fn. 124), 136 ff. und 139 ff.; *Rosenthal* (Fn. 120), Rz. 13.
153 Vgl. WP 169 (Fn. 123), 16.
154 Siehe hierzu auch *Rosenthal/Epprecht* (Fn. 124), 136 ff. und 139 ff.
155 *Rosenthal* (Fn. 118), Rz. 57.
156 Vgl. *Rosenthal* (Fn. 118), Rz. 57; ähnlich auch *Roth* (Fn. 3), 684 f.

bzw. der jeweilige Mitarbeiter, die bzw. der für die Verletzung der entsprechenden Pflicht verantwortlich ist.

V. Schlussbemerkungen

Im Kontext von Open Banking sind unterschiedliche Formen der Kooperation zwischen Bank und TTP vorstellbar. Die Autorinnen und Autoren des vorliegenden Beitrags haben anhand von vier «Muster-Kooperationsformen» die dabei entstehenden rechtlichen Beziehungen zwischen den Beteiligten untersucht und zeigen am Beispiel von spezifischen vertrags- und datenschutzrechtlichen Fragestellungen auf, wie sich diese auf die Haftung auswirken.

In vertragsrechtlicher Hinsicht trifft die Bank in jedem Fall die Verpflichtung, die für den Datenaustausch verwendeten Schnittstellen bzw. APIs genügend zu sichern, ansonsten sie unter Umständen für Vermögensschäden der Kundinnen und Kunden einstehen muss. Für die Frage, ob die Bank darüber hinaus auch für das Verhalten des TPP einstehen muss, sind die Intensität der Zusammenarbeit und die Nähe zum TPP sowie das konkrete Vertragsverhältnis zu den Kundinnen und Kunden zu berücksichtigen.

In datenschutzrechtlicher Hinsicht kommt der Bank grundsätzlich immer die Rolle als Verantwortliche zu, d.h., sie hat insbesondere die Datensicherheit zu gewährleisten. Falls der TPP (allein) über Zwecke und/oder wesentliche Mittel der jeweiligen Datenbearbeitung (mit-)entscheidet, qualifiziert er neben der Bank als (eigenständiger/gemeinsamer) Verantwortlicher und hat daher allein oder zusammen mit der Bank für die Sicherstellung der Datensicherheit zu sorgen. Falls der TPP die Kunden- bzw. Personendaten im Auftrag und nach Weisung der Bank bearbeitet, qualifiziert er als Auftragsbearbeiter. Bei einem Datenschutzverstoss kann die betroffene Person gegen jeden, der an der Persönlichkeitsverletzung mitwirkt, vorgehen – das kann sowohl der Verantwortliche als auch der Auftragsbearbeiter sein. Viele Pflichten des revDSG, wie z.B. die Informations- oder Auskunftspflicht, treffen aber nur den Verantwortlichen, wobei diese teilweise strafbewehrt sind. Das Bussenrisiko trifft dabei nicht das Unternehmen, sondern die für die konkrete Datenbearbeitung verantwortlichen Mitarbeitenden.