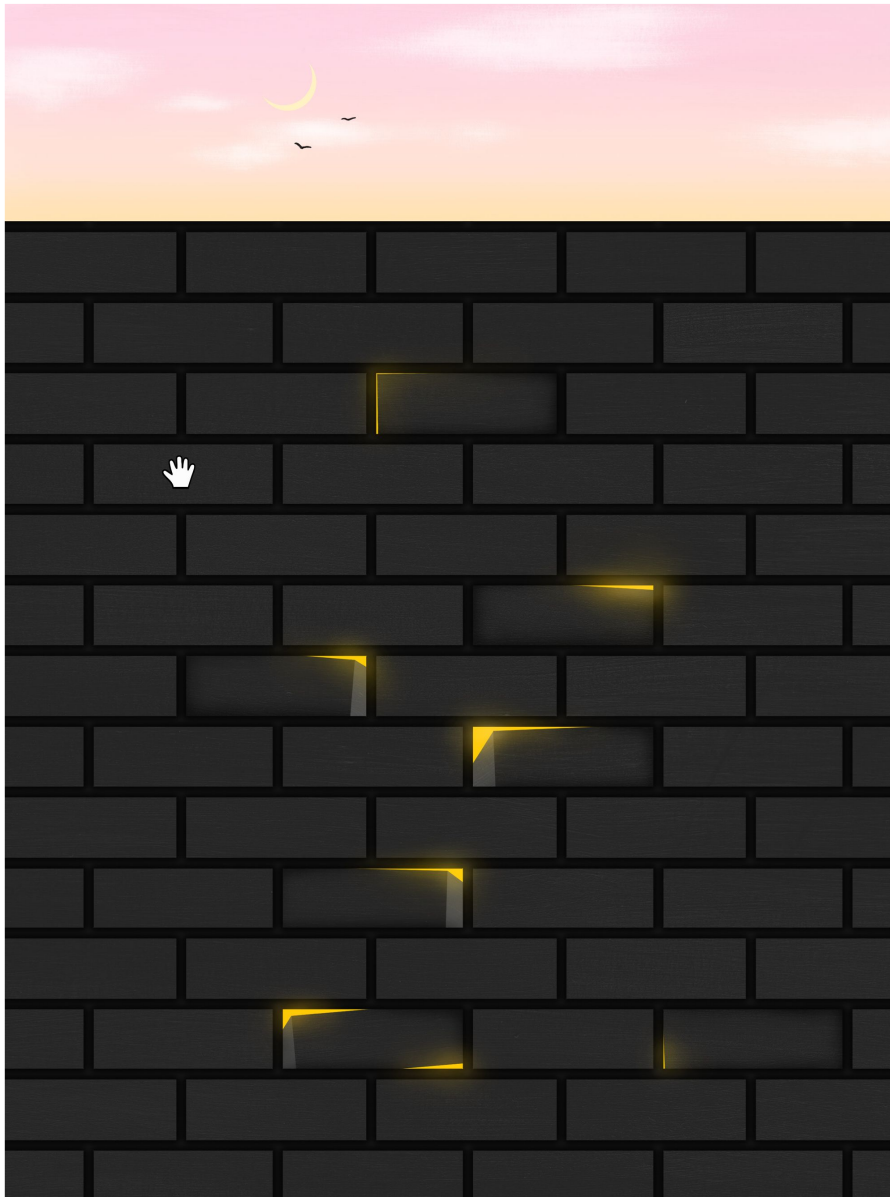

Die nicht ganz normale Bank

Eine Sicherheitslücke bei der Postfinance ermöglichte Einblick in die Daten von Kunden. Möglicherweise wurde dabei auch das Bankgeheimnis verletzt.

Eine Recherche von [Adrienne Fichter](#) (Text) und Lina Müller (Illustration), 24.02.2022



«Eine Bank, die nicht am Paradeplatz ist? – Ist doch ganz normal.»

In ihrem neuesten, mit Technobeats untermalten Werbeclip gibt sich die Postfinance betont cool. Sie will sich von den anderen Finanzinstituten ab-

heben. Eine sympathische Bank für die Kleinanlegerinnen mit bescheidenem Budget – bürgernah, trendy, das urbane Publikum ansprechend.

Ganz normal eben.

Doch wie normal ist es, dass eine Schweizer Bank Kundendaten quasi auf dem Silbertablett serviert, einsehbar für jedermann, ohne dass die Kundinnen sich in den meisten Fällen dessen bewusst sind? Genau das hat die Postfinance während längerer Zeit getan, wie eine Recherche der Republik gemeinsam mit dem Informatiker Simon Gantenbein ergeben hat.

Gegenstand der Recherche ist der Zahlungsverkehr. Die Postfinance spielt darin seit jeher eine wichtige Rolle: Sie führt Konten für ihre Kunden und erledigt Zahlungen zwischen Senderinnen und Empfängern aus der ganzen Schweiz. Datenschutztechnisch heikel ist dabei die Schnittstelle, also das Interface, in dem Zahlungen im System erfasst werden können.

Die Recherche der Republik hat folgende Probleme zutage gefördert:

1. Eine **Sicherheitslücke**: Im Onlinebanking-Portal der Postfinance konnte man sich als Kundin ohne grossen Aufwand Zugang zu Namen, Vornamen und Adressen von weiteren Postfinance-Kunden verschaffen. Im Republik-Testlauf konnten so unter anderem die Bankverbindungen von Nationalrätinnen, Regierungsräten und von einer Bundesrätin ausfindig gemacht werden. Die Bank hat die Lücke inzwischen geschlossen.
2. Ein **Datenschutzproblem innerhalb der Postfinance**: Die technischen Voreinstellungen, welche die Sicherheitslücke möglich machten, sind mutmasslich nicht vereinbar mit dem Bankkundengeheimnis. Die Bank begründet dies mit ihrem Grundversorgungsauftrag. Ob das rechtens ist, wurde bis heute von keinem Gericht beurteilt. Der eidgenössische Datenschutzbeauftragte hat rechtliche Abklärungen eingeleitet.
3. Ein **Datenschutzproblem bei anderen Banken**: Die Onlinebanking-Systeme von Migros Bank, Bank Cler, UBS sowie der Kantonalbanken von Graubünden, Schwyz, Thurgau, Schaffhausen, St. Gallen, der Waadt und Baselland haben ebenfalls Kontodaten von Postfinance-Kunden sichtbar gemacht. Dies als Folge einer weiteren Besonderheit: des Postkontoverzeichnisses.

Dass im Schweizer Zahlungsverkehr erstaunlich offen mit den Kontodaten von Kundinnen der Post umgegangen wird, könnte als Kuriosum angesehen werden – als historisches Relikt aus einer vordigitalen Zeit. Wäre da nicht das Herzstück der Schweizer Bankengesetzgebung: das Bankkundengeheimnis.

1. Die Sicherheitslücke

Wer die Onlinebanking-Lösung seiner Bank nutzt, kennt das Prozedere: Für eine Überweisung müssen neben der Kontonummer meist auch der Name und die Adresse der Empfängerin eingegeben werden. Man tippt bei der Überweisung einerseits die IBAN- oder die Postkontonummer und beim Empfängerfeld andererseits auch noch den Namen und die Adresse ein.

Typischerweise kontrolliert eine Bank anschliessend bei der Ausführung der Zahlungsanweisung, ob der zur Kontonummer gehörende Name mit der Eingabe übereinstimmt. Bei deutlichen Abweichungen wird die Transaktion gestoppt.

Im Falle einer Überweisung an ein anderes Postfinance-Konto macht es die Postfinance ihren Kundinnen hier besonders einfach: Es reicht die Eingabe der Postkontonummer. Das System ergänzt dann automatisch Namen und Adresse des Empfängers, sofern dieser das Onlinebanking der Postfinance nutzt.

Das ist praktisch, weil es den Kunden Arbeit erspart. Es bedeutet aber auch, dass bei jeder Eingabe einer gültigen Postkontonummer Name, Vorname und Adresse des entsprechenden Kontoinhabers angezeigt werden. Das verstösst womöglich gegen das Bankgeheimnis – mehr dazu später.

Zwar enthalten Postkontonummern eine Prüfziffer (man kann also nicht einfach eine beliebige sechsstellige Zahl eingeben). Doch deren Berechnung ist weder ein Geheimnis noch rechnerisch anspruchsvoll. Sie folgt der Logik einer öffentlich dokumentierten Formel.

Und so kann theoretisch jeder mit einem Zugang zum Onlinebanking der Postfinance mit etwas zeitlichem Aufwand und ein paar Zeilen Programmiercode die Kontonummern und Namen anderer Kunden ermitteln.

Simon Gantenbein, Informatiker und Vorstandsmitglied der Digitalen Gesellschaft, hatte es erfolgreich ausprobiert und das Programm auf der Plattform Github öffentlich geteilt.

Ich will es genauer wissen: Wie wurde die Datenbank mit Postfinance-Kundinnen angelegt?

Mit ein paar wenigen Zeilen Programmcode lassen sich ohne grossen Aufwand sämtliche Postkontonummern mit Onlinebanking-Zugang sowie Name und Adresse der Kontoinhaberinnen extrahieren. Damit das Programm auf das Onlinebanking der Postfinance zugreifen kann, muss man sich vor dem Start einmal wie gewohnt von Hand einloggen, anschliessend kann man entweder die Zugriffsdaten (Session-Cookie etc.) aus dem Browser auslesen oder, noch einfacher, direkt den Browser mit einem eigenen Programm fernsteuern. Für Postfinance sieht es dann einfach so aus, als ob hier ein Postfinance-Kunde sehr schnell tippte und klickte.

Die Experimente der Republik haben gezeigt, dass mit einem modernen Computer rund 36'000 Abfragen pro Stunde möglich wären, mit einem besonders leistungsfähigen sogar rund 180'000 Abfragen. Um sämtliche möglichen Kontonummern abzufragen, bräuchte man damit rund 178 Stunden (also etwas mehr als eine Woche). Diesen Computer muss man sich noch nicht mal unter den Schreibtisch stellen, sondern man kann ihn bei einem Cloud-Anbieter für ein paar Franken pro Stunde mieten.

Das Programm selbst ist dann eher trivial: Postkontonummern haben alle das Format RR-NNNNNN-C. Dabei steht RR für eine zweistellige Regionen-Nummer, NNNNNN für eine sechsstellige Laufnummer innerhalb der Region und C für die Prüfziffer. Die Regionen-Nummern beziehen sich auf die frühere Einteilung der Postregionen.

Die Prüfziffer lässt sich über einen öffentlich bekannten Algorithmus bestimmen, das Handbuch «Recordstrukturen Elektronische Dienstleistungen».

So kann das Programm sämtliche Laufnummern erzeugen, jeweils die Prüfziffer dazu berechnen und mit der so generierten Postkontonummer eine Zahlung erfassen. Falls die Nummer gültig ist, wird der zugehörige Name im entsprechenden Feld eingeblendet und kann ausgelesen und gespeichert werden.

So hat Gantenbein die Kontoangaben des Postfinance-CEO, einer Bundesrätin, von 14 von 24 Berner Nationalrätinnen, 3 von 7 Berner Regierungsräten, eines ehemaligen Chefs des Nachrichtendienstes und vieler weiterer hochrangiger Bundesverwaltungsangestellten herausgefunden. Er stoppte sein Experiment schliesslich bei 350'000 Datensätzen und meldete die Sicherheitslücke am 20. Januar 2022 der Postfinance.

Gantenbein sagt, er hätte noch viel mehr rausfinden können: «Es gibt 4,2-Millionen Konten bei Postfinance. Hätte ich mein Programm in die Cloud ausgelagert und mit voller Geschwindigkeit laufen lassen, so hätte ich in-ner zwei Wochen den kompletten Kundenstamm herunterladen können.»

Die Bank hat von dieser Aktivität offenbar nichts mitbekommen: «Ohne eine Meldung meinerseits hätte die Postfinance wahrscheinlich bis heute nicht realisiert, dass jemand massenhaft Kundendaten heruntergeladen hat.»

Gemäss Postfinance existierte die Lücke erst ab 2019. Bis dahin soll es eine Sperre für Massenabfragen gegeben haben: «Bedauerlicherweise ist dieser vor über zehn Jahren eingeführte Sperrmechanismus bei einer Weiterentwicklung von E-Finance im Jahr 2019 unvollständig aktualisiert worden», sagt Sprecher Rinaldo Tibolla. Weshalb die Sicherheitssysteme nicht Alarm geschlagen haben, begründet die Postfinance nicht genauer, sondern verweist ebenfalls auf die fehlende technische Sperre.

Immerhin: Die Postfinance hat schnell auf den Hinweis reagiert und die Lücke am 12. und 13. Februar mit einem Software-Update behoben. Massenabfragen sind seither nicht mehr möglich.

2. Das Datenschutzproblem der Postfinance

Am grundlegenden System – dass nach der Eingabe einer Kontonummer automatisch der Name des Empfängers erscheint – hält die Bank aber fest. Auch wenn sie damit nicht nur den Datenschutz, sondern auch das Bankgeheimnis ritzt.

Dieses ist im Bankengesetz ([Artikel 47](#)) und zivilrechtlich ([Zivilgesetzbuch Artikel 27](#), [Artikel 28](#)) festgeschrieben. Es schützt nicht nur sensible Informationen über das Vermögen: Bereits das Wissen um die Existenz einer Bankbeziehung, also dass eine bestimmte Person zum Beispiel ein Konto bei der UBS hat, fällt unter das Bankgeheimnis, wie aus der [einschlägigen Fachliteratur](#) hervorgeht. Genau diese Information lässt sich im Onlinebanking der Postfinance ohne grossen Aufwand eruieren.

Warum handhabt die Postfinance dies so?

Die Antwort führt zurück in die Zeit, als Überweisungen noch vorwiegend am Postschalter getätigt wurden. Die Post hat in diesem Bereich einen Versorgungsauftrag: Sie muss etwa auch Bargeld annehmen, wenn jemand eine Überweisung tätigen will. Damit dies in jedem Fall klappt, müssen Postmitarbeiterinnen die Empfängerkontodaten kennen. So können sie diese am Schalter nochmals überprüfen und dem Zahlenden bestätigen.

Diese Logik wurde aus dem Analogen ins Digitale übertragen. Zwar ohne Postangestellte als Mittlerinnen, aber mit dem primären Auftrag, dass alles unternommen werden muss, um Falschzahlungen und Rückweisungen zu verhindern. Dieser historisch bedingte Sonderfall wird als «Konto-

öffentlichkeit» bezeichnet. Er führt dazu, dass die Postfinance sich selbst als Spezialfall unter den Banken sieht.

Verletzt die Kontoöffentlichkeit nicht das Bankgeheimnis? Die Postfinance delegiert diese Frage an ihre Kunden. «Massgeblich ist hier die Frage, ob die Kundinnen und Kunden in eine Einschränkung einwilligen können. Dies ist grundsätzlich der Fall», sagt Postfinance-Sprecher Tibolla. «Bevor Postfinance eine eigenständige Aktiengesellschaft wurde und der Finma unterstellt wurde, hatte Postfinance die Kontoöffentlichkeit eingehend geprüft.»

In der Tat pflegte die Postfinance mit dem Bundesamt für Justiz und der Eidgenössischen Finanzmarktaufsicht (Finma) zu dieser Frage einen intensiven Austausch. Beide Ämter wollen sich heute nicht mehr zum Fall äussern. Finma-Sprecher Tobias Lux sagt: «AGB sind Bestandteil der zivilrechtlichen Vertragsbeziehung zwischen den Banken und ihren Kunden und werden somit grundsätzlich nicht von der Finma geprüft oder genehmigt.»

Das Resultat der «eingehenden Prüfung» durch die Behörden ist ein Merkblatt mit den wichtigsten Fragen und Antworten, das Postfinance-Kunden mit den Allgemeinen Geschäftsbedingungen (AGB) bei der Eröffnung eines Kontos erhalten. Es trägt den Namen «Handhabung des Bankkundenheimnisses bei der Postfinance AG».

So weit, so gut. Problematischer ist eine andere Stelle im Merkblatt:

Kann jedermann ohne Weiteres in Erfahrung bringen, ob und welches Konto ich bei der Postfinance AG habe? Nein. Am Schalter sollen unsere Mitarbeitenden die Angaben für eine Einzahlung oder Überweisung nur ergänzen oder korrigieren können. Zudem können Sie selber im E-Finance prüfen, ob eine eingegebene Kontonummer zum richtigen Zahlungsempfänger gehört, um Falschzahlungen auszuschliessen. (...)

Mit dem letzten Satz wird die Frage im Grunde bejaht: Jedermann kann «in Erfahrung bringen, ob und welches Konto ich bei der Postfinance AG habe». Denn wer Geduld mitbringt, kann die Postkontonummern manuell nacheinander ausprobieren, sofern er die Logik dahinter kennt. Oder dies technisch erledigen lassen (wie in der Box weiter oben erklärt).

Die automatische Anzeige von Postfinance-Kontodaten wird auch mit einem Verweis auf die Allgemeinen Geschäftsbedingungen legitimiert. Darin ist von einer «Ergänzung von Empfängerkoordinaten im E-Finance bzw. für Schalterauskünfte» die Rede.

Brisant dabei: Es gibt kein sogenanntes Opt-out zur automatisierten Datenergänzung, wie Sprecher Tibolla bestätigt. Das heisst, Postfinance-Kunden haben nicht die Möglichkeit, die Anzeige ihrer Daten zu deaktivieren.

Kurzum: Die Bank hält nach dem Sicherheitsvorfall an ihrem Service fest. Auch wenn dies dem datenschutzaffinen Teil ihrer Kunden nicht gefallen dürfte und Fragen hinsichtlich des Bankgeheimnisses aufwirft.

Doch das letzte Wort ist noch nicht gesprochen. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte Adrian Lobsiger hat Abklärungen eingeleitet: Er tauscht sich zurzeit mit Postfinance darüber aus, «ob das Unternehmen die auf eine Einwilligung in den AGB gestützte Datenergänzung mit der Möglichkeit eines Opt-out ergänzen wird».

Monika Roth, eine Juristin mit Spezialgebiet Bankenrecht, äussert sich ebenfalls kritisch. «Eigentlich wird das Bankgeheimnis von Postfinance to-

tal ausgehebelt.» Der Wortlaut im Bankengesetz sei eindeutig: «Der Verstoß gegen das Bankkündengeheimnis ist ein Officialdelikt, und es sieht eben keine Ausnahme vor im Sinne: Bank mit Grundversorgungsauftrag ist davon ausgenommen.»

Roth hält die Praxis der Postfinance für ungenügend legitimiert: «Es bräuchte eine ausdrückliche gesetzliche Grundlage, die den Anliegen der Postfinance im Rahmen der Grundversorgung und des Zahlungsverkehrs Rechnung trägt.»

Ich will es genauer wissen: Können sich Banken durch AGB vom Bankgeheimnis entbinden lassen?

In der Literatur ist allgemein die Handhabung durch AGB und «informierte Einwilligung» zum Verzicht des Bankkündengeheimnisses umstritten. Vieles hängt von der Qualität und Transparenz vonseiten der Bank ab, etwa ob die Klausel grafisch hervorgehoben ist.

Zum einen ist dieser Verzicht durchaus zulässig, wie Frédéric Krauskopf, Professor für Privatrecht an der Universität Bern, bestätigt: «Das Bankgeheimnis gilt nicht absolut. Es darf mit Einwilligung der Bankkundin beziehungsweise des Bankkunden beschränkt oder aufgehoben werden.» Politisch hat das auch der Bundesrat festgehalten, in einer kurzen Antwort auf die Frage von SVP-Nationalrat Gregor Rutz, ob das Bankgeheimnis per AGB ausgeschaltet werden könne: «Für die Einwilligung stellt das Gesetz keine Formvorschriften auf. Sie kann grundsätzlich auch im Rahmen von AGB erteilt werden.»

Auf der anderen Seite handelt es sich dabei laut Krauskopf um eine eher «ungewöhnliche Klausel». Denn: «Das Bankgeheimnis an sich gehört zum Kern der Geschäftsbeziehung zwischen der Bank und ihren Kundinnen und Kunden.» Eine andere Frage ist jedoch, «ob die fragliche AGB-Klausel für Bankkundinnen und Bankkunden nicht ungewöhnlich ist, da diese den AGB in aller Regel global zustimmen, also ohne diese im Einzelnen gelesen (und verstanden) zu haben». Hier ist die Bank in der Beweispflicht, wie das Urteil des Bundesgerichts zu einem Versicherungsfall zeigt.

Doch vor einem Gericht würden solche AGB wohl nicht standhalten, wie Aussagen von befragten Bankrechtsprofessoren und ein Blick in die Fachliteratur bestätigen. Auch der Bundesrat schreibt: «Die Beurteilung, ob eine solche Einwilligung im Einzelfall inhaltlich rechtsgenügend erfolgt, obliegt den zuständigen Gerichten.»

Kurz: Wo keine Klägerin, da kein Richter. Niemand hat bisher das Thema AGB und Bankgeheimnis seit der Übernahme des automatischen Informationsaustauschs angetastet.

Der Datenschutzbeauftragte Adrian Lobsiger erachtet die Unterlagen der Postfinance jedoch als genügend: «Das Merkblatt gibt Auskunft darüber, welche Daten an wen und zu welchen Zwecken weitergegeben werden. Damit werden die wichtigen Informationen erteilt.» Professor Krauskopf sagt, dass es zwar durchaus ausreichend informiere, «für mich allerdings nicht erkennbar ist, ob das Merkblatt neben den AGB auch Vertragsbestandteil ist oder wird».

3. Das Datenschutzproblem bei anderen Banken

Die Republik hat auch im Onlinebanking anderer Schweizer Banken geprüft, ob Namen und Adressen von Kundinnen automatisch

vervollständigt werden. Insbesondere hat uns die Handhabung von Postfinance-Empfängerkonten interessiert.

Dabei hat sich gezeigt, dass die meisten Banken den Datenschutz streng auslegen. Bei einer neuen Überweisung werden nicht automatisch Angaben zur Empfängerin ergänzt – egal von welcher Bank. Alle Angaben wie Namen und Adresse müssen von Hand selbst eingetippt werden.

Doch es gibt ein paar Ausnahmen.

Zu ihnen zählen etwa die Schwyzer, die Schaffhauser und die Bündner Kantonalbank. Sie ergänzen automatisch Kontoangaben von privaten und geschäftlichen Postfinance-Empfängerkonten. Im Prinzip handelt es sich dabei um den gleichen Datenschutz-Missstand wie bei der Postfinance. Mit dem gewichtigen Unterschied aber, dass die Postfinance-Kundinnen gar keine direkte Vertragsbeziehung mit diesen drei Kantonalbanken haben.

Ein ähnliches Problem besteht bei der Thurgauer und der St. Galler Kantonalbank: Auch sie ergänzen teilweise die Namen und Adressen von Privatkunden der Postfinance.

Weniger problematisch gehen die Migros Bank, Bank Cler, UBS und die Kantonalbanken von Baselland und der Waadt vor. Sie pflegen einen «Zusatzdienst», in dem sie bei vielgenutzten Postfinance-Konten von Geschäftskundinnen – etwa Versicherungen, Krankenkassen, Telecomunternehmen – die Adressangaben *as a service* vervollständigen.

Auf die Frage, woher die Banken diese Postfinance-Daten haben, schreibt eine Sprecherin der St. Galler Kantonalbank: «Es handelt sich um eine Teilmenge des Datenbestands, welchen Postfinance in ihrer E-Finance-Lösung anbietet.»

Auch hier geht es um eine historisch bedingte Eigenheit: das Postkontoverzeichnis. Dieses lag bis in die 1990er-Jahre an den Postschaltern sogar öffentlich in Papierform auf. Jeder Filialbesucher konnte alle Postkontoangaben von jeder Person einfach einsehen. Diese «Gelben Seiten für Postkonten» wurden dann in den digitalen Zahlungsverkehr mit anderen Banken übernommen.

Die Postfinance hat die Sache mit dem Kontoverzeichnis transparent gekennzeichnet und verlangt dafür ein Opt-in, wie Sprecher Tibolla auf Anfrage erklärt: «Neben dem Merkblatt erhalten Kundinnen und Kunden bei der Kontoeröffnung ebenfalls ein Formular, wo anzukreuzen ist, ob man Teil des Kontoverzeichnisses sein möchte oder nicht.»

Aber wem ist schon klar, dass mit einem Eintrag ins Kontoverzeichnis eigene Daten automatisch zu fremden Banken wandern?

«Die Einwilligung der Postfinance über die AGB ist eine Farce», sagt Franziska Ryser, Nationalrätin der Grünen. «Wenn Kundinnen diese unterschreiben, wissen sie nicht, dass ihre Kontoinformationen in ein Register eingetragen und jedem online dargestellt werden.»

Im bereits erwähnten Merkblatt der Postfinance steht lediglich als letzter Punkt, dass man sich aus dem Kontoverzeichnis wieder austragen lassen könnte. Doch wie viele Postkunden haben das effektiv getan? Man messe nicht, wie viele Kundinnen sich wieder austragen liessen, sagt Sprecher Tibolla.

Immerhin: Dieser Zusatzservice der Postfinance für alle anderen Banken ist seit kurzem Geschichte. Das Kontoverzeichnis wurde gemäss Angaben der Bank am 12. und 13. Februar 2022 eingestellt – am gleichen Wochenende also, an dem die Sicherheitslücke geschlossen wurde. Das sei Zufall, sagt Tibolla, es habe nichts mit den Recherchen von der Republik und von Simon Gantenbein zu tun.

Löst der QR-Code das Problem?

Informatiker Simon Gantenbein hat den Datensatz inzwischen gelöscht. In seinem Bericht zählt er auf, was er damit hätte anstellen können. «So hätten die kantonalen Steuerbehörden meine Datensammlung sicher genommen, um damit den Erinnerungslücken der Steuerbetrüger gezielt entgegenzuwirken», sagt er der Republik. «Die Datensammlung könnte auch mit weiteren Datenquellen verknüpft werden. Dies hätte Phishing-Angriffe oder Identitätsdiebstahl begünstigt.»

Fast unisono versicherten alle befragten Banken, dass sich die Problematik von selbst erledigen werde: mit einer neuen Rechnungsform ab Herbst 2022. Damit werden die alten Einzahlungsscheine abgeschafft und durch QR-Codes ersetzt, die sämtliche gescannten Daten elektronisch übermitteln. Der «Automatisierungsservice» erübrige sich.

Auch die Postfinance prüfe eine allfällige Abschaffung ihres Automatisierungsdienstes im Zuge dieses Wechsels, sagt Sprecher Tibolla. Damit würde die Post-Tochter in diesem Punkt doch nachgeben.

Gleichzeitig arbeitet Franziska Ryser auf politischer Ebene an einer Abschaffung der Praxis. Als Mitglied der Kommission für Wirtschaft und Abgaben zieht die Grünen-Nationalrätin einen Vorstoss in Betracht: «Wir prüfen, ob eine Opt-in-Lösung hierfür zielführend ist», sagt sie. «Kundinnen müssten aktiv der Weitergabe ihrer Daten zustimmen.»

Informatiker Gantenbein begrüsst das: «Es sollte für Banken selbstverständlich sein, dass bei der Nutzung von personenbezogenen Daten, zum Beispiel für Marketingzwecke oder zur Ergänzung von persönlichen Daten in einer Zahlung, um explizite Erlaubnis bei der Kundschaft gebeten wird.»

Ob alle Bankkundinnen bald nur noch mit Smartphone und QR-Code zahlen werden, ist allerdings fraglich. Es werden wohl noch viele Nutzer weiterhin via Desktop und Notebook die Rechnungen einzahlen und diese manuell eintippen, inklusive Automatisierungsservice.

Fazit: Nach aussen sind die Kundinnen der Postfinance nun besser geschützt. Doch innerhalb der Bank bleiben sie für andere Kunden – vorerst – gläsern. Und das wegen eines Automatisierungsservice, der historisch begründet wird und womöglich das Bankkundengeheimnis verletzt.

Die Postfinance bleibt alles andere als eine ganz normale Bank.