DIE EVOLUTION DER GEGENSÄTZE – SPANNUNGSFELD BETRUGS- UND GELDWÄSCHE-BEKÄMPFUNG VERSUS DATENSCHUTZ?

Renate Riedl / Markus Kemptner

Renate Riedl, Senior Privacy Manager, Paysafe Group, Privacy
Am Europlatz 2, 1120 Wien, AT
renate.riedl@paysafe.com

Markus Kemptner, Head of Financial Crime Analytics, Paysafe Group, Compliance
Am Europlatz 2, 1120 Wien, AT
markus.kemptner@paysafe.com

Schlagworte: ***Financial Crime, Geldwäsche, Onlinebetrug, eCrime, eMoney, Datenschutz, Datenminimierung***

Abstract: *Während in der Bekämpfung von Geldwäsche und Betrug ein «Mehr an Daten» und ein exponentielles Ansteigen der Datenquantität notwendig ist, um effektiv vorgehen zu können, sind die Anforderungen im Datenschutz durch Datenminimierung und Wahrung der Rechte der Betroffenen scheinbar im Widerspruch dazu. Der Begriff des Personenbezuges ist dabei ein zentraler Punkt in der Beurteilung und Auswahl der Methodik. Dabei sind der Bereich Finanzkriminalität als auch der Datenschutz in der Entwicklung geprägt von einer Hinwendung zum risikobasierten Ansatz. Der Beitrag widmet sich der Schnittstelle aus Sicht der Praxis im Online-Zahlungsverkehr und beleuchtet die Herausforderungen.*

1. Einleitung

Ziel dieses Artikels ist es, einen praxisbezogenen Einblick in die Methoden bei Betrugs- und Geldwäschebekämpfung sowie der Bekämpfung von Terrorismusfinanzierung und zu den vermeintlich damit im Spannungsfeld stehenden Anforderungen des Datenschutzes zu bieten. Veranschaulicht wird dies am Beispiel des Online-Zahlungsverkehrs. Dabei wird im ersten Teil das Umfeld der Erkennung und Bekämpfung erläutert, während darauf aufbauend einige Problemstellungen bei der datenschutzrechtlichen Problematik umrissen werden.

2. Financial Crime als Überbegriff von Betrug und Geldwäsche

Der Begriff financial crime soll hier als Überbegriff von Geldwäsche, Betrugs- und Terrorismusfinanzierung fungieren. Umgangssprachlich werden die Begriffe Betrug und Geldwäsche oftmals synonym verwendet. Aus Sicht des Finanzdienstleisters gibt es hier aber einen eklatanten Unterschied. Betrug bedeutet für den Finanzdienstleister durchaus realen finanziellen Verlust. Sei es zur Schadloshaltung des Kunden oder durch Betrug am Finanzdienstleister selbst. Geldwäsche hingegen bedeutet keinen unmittelbaren finanziellen Schaden für den Finanzdienstleister, sondern – solange unbemerkt – durch hohe Transaktionsvolumen mitunter sogar Gewinne.

Das Risiko unbemerkter Geldwäschetransaktionen ist vielmehr indirekter Art und spiegelt sich in Reputationsschaden, systemischem Schaden oder Strafzahlungen wider. Betrug ist dementsprechend für den Finanzdienstleister klar definierbar, da ein direkter Schaden entsteht. Geldwäsche hingegen ist in den allermeisten

Fällen nur das Entstehen eines Verdachtsfalles und wird erst durch abnormes Transaktionsverhalten erkennbar.

Prüfung und Erarbeitung von Gegenmaßnahmen in diesem Bereich sind im Online-Zahlungsverkehr oftmals sehr ähnlicher Natur, was hier als Kernthema dieses Artikels genauer behandelt wird. Heute entscheiden sich vor allem Online-Zahlungsdienstleister vermehrt für eine begriffsübergreifende financial crime prevention Strategie[1]. Diese wird strategisch abseits der umsatzmotivierten Konzernstränge beispielsweise in den Rechtsabteilungen oder im Compliance-Bereich angesiedelt. So dient eine Organisationsstruktur bei größeren Finanzdienstleistern vor allem dazu, die Umsetzung entsprechender (vermeintlich) gewinnreduzierender Maßnahmen zu erleichtern, da diese Abteilungen in der Regel unabhängig von Wachstums- oder Gewinnvorgaben agieren und primär der Einhaltung von gesetzlichen Vorgaben und einer Risikominimierung dienen.

3. Kenne deinen Kunden

Nach wie vor besteht in der Banken- und Finanzlandschaft und auch beim Gesetzgeber das unumstößliche Credo der Kundenverifikation[2], im Fachjargon und auch hier im Artikel nachfolgend als KYC («Know Your Customer») bezeichnet. In der Praxis bedeutet dies eine Verifikation mittels eines offiziellen Dokuments, sowie dessen Abgleich mit dem realen Erscheinungsbild des Kunden. Im Gegensatz zur «brick and mortar»[3] Zahlungsindustrie, wo der Kunde persönlich in einer Bankfiliale vorstellig werden muss, wird dies im Online-Zahlungsverkehr durch den Abgleich möglichst aktuellen Bildmaterials, zum Beispiel im Zuge der Videoverifikation oder mittels Fotos des Kunden durchgeführt. Im Laufe der Geschäftsbeziehung und des Geschäftsgebarens wie etwa bei geldintensivem Transaktionsverhalten wird die Kundenverifikation fortgeführt und inhaltlich erweitert. Dazu bedient man sich Einkommensnachweisen, Steuererklärungen und ähnlicher Nachweise zur Belegung des Geldursprungs.

Diese Daten bilden historisch die Ausgangsbasis der Datenlage für financial crime investigation und prevention, also sowohl für die Verfolgung von Straftaten als auch für die Prävention. Ermittlungen im Zuge einer kriminellen Handlung dienen der Identifizierung des/der Täter/s und deren strafrechtlicher Verfolgung. Ähnlich kann diese Maßnahme auch als Präventionsmaßnahme gewertet werden, da mitunter bereits durch die Aufhebung der Anonymität die Hemmschwelle für den Betrug angehoben wird.[4]

Begeht ein Kunde eine kriminelle Handlung, versucht er in der Regel sich einer Überführung zu entziehen indem er die Identifizierung verhindert (etwa durch Stückelung der Transaktion, um unter der Grenze zur verpflichtenden Verifikation zu bleiben) oder sabotiert (etwa durch gefälschte Dokumente oder gestohlene Identitäten – siehe unten).

Im Online-Zahlungsverkehr ist die Aufhebung der Anonymität eine unzulängliche Maßnahme, um organisierten Gruppen und Personen mit erhöhtem kriminellem Potential das Handwerk zu legen. Gestohlene oder gefälschte Identitäten sind sehr leicht mittels diverser Software zu erstellen bzw. manipulieren oder über das Internet zu erwerben.[5]

---

1 Curry, Frederic. (02. 04 2019) Financial Crime and Organizational Structure (D. US, Interviewer) CFO Innovation. von https://www.cfoinnovation.com/risk-management/financial-crime-and-organizational-structure, abgerufen am 03. 12. 2019.

2 Erwägungsgrund 22 in Richtlinie (EU) 2018/843 des Europäischen Parlaments und des Rates vom 30. Mai 2018 zur Änderung der Richtlinie (EU) 2015/849 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung und zur Änderung der Richtlinien 2009/138/EG und 2015/849/EG, ABl. L 156/43.

3 Pritchard, Justin, (09. 08. 2019) Brick and Mortar Bank Branches. Über die Balance: https://www.thebalance.com/brick-and-mortar-what-does-it-mean-315467, abgerufen am 03. 12. 2019.

4 Janssen, Gerhard. (2012). Betrug. In: Achenbach, Hans/Ransiek, Andreas (Hrsg.), Handbuch Wirtschaftsstrafrecht[3], S. 523–587.

5 The United States Department of Justice, (07. 02. 2017), What are Identity Theft and Identity Fraud, The United States Department of Justice: https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud, abgerufen am 1. 12. 2019.

Hinzu kommt die steigende Geschwindigkeit in der Verarbeitung von Transaktionen und die zunehmende Internationalisierung im Online-Zahlungsverkehr.[6] Transaktionen werden innerhalb von Sekunden von einem Finanzsystem in das nächste geschleust. Bei organisierten kriminellen Gruppen meist durch Missbrauch internationaler Zahlungsdienstleister und über nationale Grenzen hinweg. Oftmals auch über sogenannte money mules[7], oder Konten, die nur für kurze Zeit und ausschließlich für den Zweck der Verschleierung («layering»)[8] erstellt und genutzt werden.

4. Erkenne deinen Kunden und erkenne einen Betrüger

Die Kundenverifikation als alleinstehende Maßnahme ist unzureichend, um den Kunden zu «kennen» und financial crime effektiv erkennen, verfolgen und verhindern zu können. Es bedarf mehr, als den Kunden nur zu verifizieren, um das Kundenverhalten und Beweggründe für sein konkretes Verhalten schlüssig nachvollziehen zu können.

Kernaufgabe der financial crime prevention ist es folglich, das Verhalten krimineller Individuen vom Verhalten regulärer Kunden unterscheiden zu können. Das führt unweigerlich zu der Notwendigkeit in einem ersten Schritt, die jeweiligen Verhaltensmuster und insbesondere dasjenige von Kriminellen zu erkennen und zu klassifizieren. In einem zweiten Schritt ist es notwendig dieses Verhalten aus der Vielzahl von Transaktionen herauszufiltern. Oder anders herum gesagt – das gewünschte und/oder erwartete Kundenverhalten zu definieren, um dann ein abweichendes und potenziell kriminelles Verhalten erkennen zu können.

Hier spielt besonders ein Faktor in der financial crime prevention eine zentrale Rolle: die Wiederholung und dadurch entstehende Muster: Kriminelle Individuen sowie organisierte kriminelle Gruppen neigen zum Zweck der Effizienzsteigerung dazu, bewährte Strategien zu wiederholen. Dies erscheint im Online-Finanzsektor auch deshalb einfach, weil der persönliche Kontakt zwischen Kunden und Finanzdienstleister nicht mehr stattfindet[9]. Gerade dieser Faktor bietet in der Analyse die Möglichkeit verdächtige Transaktionen auf Basis wiederkehrender Muster hervorzuheben. Aufgrund der oben genannten Herausforderungen reicht es aber nicht aus, sich nur auf Muster im Zahlungsverhalten zu beschränken. Oftmals kommt es vor, dass in einem komplexen Geldwäsche-Zyklus[10] nur ein Teil davon über einen Finanzdienstleister abgedeckt ist oder abgewickelt wird. Dieser sieht entsprechend nur einen Ausschnitt, oftmals auch nur eine einzelne Transaktion, die ohne zusätzliche Informationen noch keine Rückschlüsse zulässt oder Muster preisgibt.

Ein vereinfachtes Beispiel wäre es etwa, wenn kriminelle Gruppen oder Individuen zum Zweck der Verschleierung Geldtransfers in mehrere Einzeltransaktionen zerlegen und für jede dieser Transaktionen eine andere Identität verwenden. Diese Einzeltransaktionen könnten beispielsweise durch die Verwendung gemeinsamer IP-Adressen zu einem größeren Muster zusammengeführt werden und auf Basis dessen kann ein Finanzdienstleister Präventivmaßnahmen setzen.

---

6 McKinsey & Company, Global Payments Report 2019: Amid sustained growth, accelerating challenges demand bold actions. McKinsey & Company (2019) https://www.mckinsey.com/~/media/McKinsey/Industries/Financial%20Services/Our%20Insights/Tracking%20the%20sources%20of%20robust%20payments%20growth%20McKinsey%20Global%20Payments%20Map/McK-2019-Global-Payments-Report.ashx, S 6, abgerufen am 04.12.2019.

7 DeSantis, Matthew, Dougherty, Chad, McDowell, Mindi (2011) US-Cert. von Understanding and Protecting Yourself Against Money Mule Schemes: https://www.us-cert.gov/sites/default/files/publications/money_mules.pdf, abgerufen am 03. 12. 2019.

8 Cox, Dennis, Handbook of Anti-Money-Laundering, John Wiley & Sons. New Jersey, 2014, S. 15.

9 Kasneci, Gjerji. (26. 09. 2017). «Bereits bekannte Betrugsmuster werden durch die Anonymität im Netz vereinfacht.». (Bankingclub, Interviewer) von https://www.bankingclub.de/news/fraudmanagement/bereits-bekannte-betrugsmuster-werden-durch-die-anonymitaet-im-netz-vereinfacht/, abgerufen am 04. 12. 2019.

10 Cox, Dennis, Handbook of Anti-Money-Laundering, John Wiley & Sons. New Jersey, 2014, S 15.

5. Das «Katz und Maus Spiel» bei der financial crime prevention

Gerade organisierte Gruppierungen verfügen über ausreichende Mittel, um binnen kürzester Zeit zu erkennen, auf welcher Grundlage Präventivmaßnahmen basieren. Ressourcen werden außerdem dazu genutzt, laufend Lücken in Präventionssystemen zu entdecken. Beim oben genannten Beispiel wäre etwa der nächste Schritt, die Nutzung von VPN[11] oder TOR Netzwerken[12]. Dies führt auf der Seite des Finanzdienstleisters wiederum zur Notwendigkeit der genaueren Analyse von IP-Metadaten, um die Nutzung von VPN oder TOR Netzwerke überhaupt feststellen zu können. Neue Daten werden herangezogen, neue Präventivmaßnahmen gesetzt, neue Lücken darin gefunden was wiederum zu neuen Mustern im Verhalten der Betrüger führt. Und das Spiel beginnt von vorne...

6. Die Potenzierung der notwendigen Datenmenge

Es ist nachvollziehbar, dass die Quantität an Daten, die durch Transaktionsüberwachung/monitoring generiert werden und zur Erkennung und Prävention von financial crime herangezogen werden können, stetig im Wachsen begriffen ist. Immer mehr Kategorien von Daten werden zur Durchführung financial crime Verfolgung un Prävention notwendig. Waren es anfangs bei KYC eine Handvoll Daten (z.B.: Name, E-Mailadresse, etc), werden heute schon «big data»[13] Strategien angewendet.

Dies reicht von IP-Daten und Metadaten über device fingerprints[14] bis hin zu Verhaltensbiometrie-Methoden, wie zum Beispiel die Analyse von Mausbewegungen[15]. Erst die Nutzung dieser Daten ermöglicht es, aus einzelnen Transaktionen ein größeres Bild zu schaffen und diese in der Folge bestimmten Mustern zuordnen zu können.

Lange Zeit waren die Täter durch dieses System von «auf Aktion folgt Reaktion» logischerweise den Finanzdienstleistern immer einen Schritt voraus. Dies initiierte in der financial crime prevention eine Trendwende weg von der transaktionsbasierten Analyse hin zu Profilbildung, die in den vergangenen Jahren zunehmend zum Erfolg geführt hat.

Die gesamte Datenmenge und Metadaten zu einer Transaktion werden mittels zusätzlicher Kalkulationen angereichert. Es werden Profile um verschiedene Basisdaten herum aufgebaut. So können zusätzliche Daten und Profile generiert werden. Berechnungen beispielsweise zu einer IP-Adresse ermöglichen damit Bewertungen wie etwa: «Wie viele Konten wurden mit einer IP-Adresse bedient?»; «In welche Länder wurde von einer IP-Adresse, Geld transferiert?»; «Wie viele Kreditkarten wurden mit einer IP-Adresse benutzt?».

Gleichermaßen können ähnliche Profile nicht nur um eine IP-Adresse herum aufgebaut werden, sondern um jede beliebige Entität, wie ein Konto, bestimmte Endgeräte oder sogar breitere Klassifikatoren wie eine E-Mail-Domain. Diese Profile werden dann genutzt, um Risikoprofile zu generieren und auf Basis der Bewertung des Risikos Entscheidungen zu treffen. Diese Herangehensweise erschwert es einem Täter, eine Lücke im System ausfindig zu machen, da der Finanzdienstleister in der Prävention proaktiv ein Risikoprofil erstellt, anstatt reaktiv eine bekannte Lücke zu schließen.

Um die Analyse von Mustern und den Einsatz von Präventionsmaßnahmen effizienter zu gestalten, wird bei den Finanzdienstleitern vermehrt auch *machine learning* eingesetzt. Hierbei werden aus den großen Daten-

[11] Norton by Symantec (2019) Privacy,What Is a VPN?: https://us.norton.com/internetsecurity-privacy-what-is-a-vpn.html, abgerufen am 03. 12. 2019.

[12] The Tor Project Inc, 2019, https://2019.www.torproject.org/about/overview.html.en, abgerufen am 03. 12 2019.

[13] Oracle, What is big data? von Big Data: https://www.oracle.com/big-data/guide/what-is-big-data.html, abgerufen am 04. 12. 2019.

[14] Cao, Yinzhi, Li, Song & Wijmans, Erik (2017). (Cross-)Browser Fingerprinting via OS and Hardware Level Features. Proceedings of Network & Distributed System Security Symposium (NDSS). Von Yinzhi Cao: http://yinzhicao.org/TrackingFree/crossbrowsertracking_NDSS17.pdf, abgerufen am 13.12.2019.

[15] Worldwide Patentnr. WO2004097601A1, 2014.

mengen automatisiert die relevantesten Kombinationen an Datenfeldern und aggregierten Daten selektiert, die am treffsichersten die Transaktions- und Verhaltensmuster krimineller Aktivitäten beschreiben[16].

7. Die «Distanzierung» vom Personenbezug

Trotz der rasanten und eklatanten Zunahme der Datenmenge, die im Zahlungsumfeld generiert und verarbeitet wird, hat sich dennoch der Fokus in Bezug auf die Typologie der Daten stark verändert. Im Unterschied zum ursprünglichen KYC, wo die Daten an sich die notwendige Information war, entwickelte sich der Fokus hin zur Mustererkennung. Dies hat zur Folge, dass die Daten für einen Analysten oder die für machine learning verwendeten Algorithmen irrelevant werden. Wichtiger ist es, die Wiederholung eines Datensatzes in den Fokus bei der Analyse zu rücken. Die für Analysten oder Algorithmen relevanten Daten, «distanzieren» sich immer mehr von einer konkreten realen Person. Der Name, das Geburtsdatum, die IP-Adresse, …: diese Daten verlieren in der financial crime prevention an Bedeutung – bis zu dem Moment, an dem dann tatsächlich ein begründeter Verdacht auf kriminelles Verhalten entsteht. Es sind vielmehr Metadaten und Kalkulationen um diese Daten herum, die die Erkennung von Auffälligkeiten, Hoch-Risiko-Transaktionen oder potentiellen Verdachtsfällen erlauben. Ein Token[17] als eine der Methoden der Pseudonymisierung für diese Daten würde ausreichen, um diese Analyse- und Präventionsnahmen umzusetzen. Erst wenn ein ausreichender Verdacht besteht, wäre die Notwendigkeit gegeben, diesen Token in tatsächlichen Daten zurückzuführen. Der nicht definierte Begriff einer «Distanzierung» vom Personenbezug und die Änderung des Fokus in der Analyse werfen die Frage auf, wie rechtlich damit umzugehen ist, bzw. welche Schranken/Herausforderungen damit verbunden sind.

8. Datenschutzrechtliche Grundlagen und Rahmenbedingungen

Grundlage der financial crime prevention sind personenbezogen Daten und damit ist die Datenschutz-Grundverordnung (nachfolgend: DSGVO)[18], neben Geldwäsche-Richtlinien und anderen rechtlichen Rahmenbedingungen die zentrale Norm bei der rechtlichen Beurteilung der Zulässigkeit der Datenverarbeitung.

8.1. Grundsätze bei der Datenverarbeitung

Die DSGVO legt in Art 5 eine Reihe von Grundsätzen fest, welche bei jeder Verarbeitung von personenbezogenen Daten eingehalten werden müssen. So sind neben Rechtmäßigkeit, Zweckbindung, Richtigkeit, Integrität und Vertraulichkeit, insbesondere die Datenminimierung und die Speicherbegrenzung eine besondere Herausforderung bei der financial crime prevention.[19]

Wie unter Pkt 7 erläutert, hat sich im Zuge der Betrugserkennung die Notwendigkeit herauskristallisiert, immer mehr an Daten zu verarbeiten[20] und für eine Mustererkennung heranzuziehen. Dabei gibt die DSGVO vor, dass Daten dem Zweck angemessen und erheblich, sowie auf das für die Zwecke der Verarbeitung – hier: Bekämpfung von Online-Betrug – notwendige Maß beschränkt sein muss. Die DSGVO sieht also vor, so

---

16 Sudjianto, Agus, Nair, Sheela, Yuan, Ming., Zhang, Aijun, Kern, Daniel & Cela-Díaz, Fernando, Statistical Methods for Fighting Financial Crimes. Technometrics, 2017, S 5–19.

17 Wex Inc. (27. 07. 2017) Tokenization 101: Understanding the Basics: https://www.wexinc.com/insights/blog/corporate-payments-edge/credit-card-tokenization-basics/, abgerufen am 04. 12. 2019.

18 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.

19 Art 5 DSGVO.

20 Der Anstieg der Datenquantität, der bereits aus der technischen Entwicklung entsteht ist, ist im KI-Bereich virulent. Siehe etwa Bonstedt, Jan; Vom Personenbezug zum Gerätebezug – KI und Datenschutz. In: Die Macht der Daten und der Algorithmen. Regulierung von IT, Iot und KI, S 413.

wenig Daten wie möglich und nur so viel wie nötig, während financial crime prevention mit einem exponentiellen Anstieg der Datenmenge dazu (scheinbar) im Widerspruch steht.

Die Festlegung, was für den konkreten Zweck als notwendig zu erachten ist, hat kein fixes Limit, sondern ist fließend und jeweils an die vorhandene Technik wie auch die Entwicklung der Betrugsmuster gekoppelt. Eine laufende Prüfung der Methodik der financial crime prevention unter Beachtung des Grundsatzes der Datenminimierung ist damit einer der Eckpfeiler bei einer risikobasierten Bewertung.

Weiterer zu beachtender Grundsatz ist die Speicherbegrenzung, wobei Daten in einer Form gespeichert werden müssen, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.[21] Gerade die Profilbildung und Musterkennung stellt dabei die Finanzbranche, und auch andere Dienstleister im e-commerce Bereich, vor die Herausforderung[22], dass Muster erst nach einem nicht klar festzulegenden Zeitraum überhaupt erst erkennbar sind. Hier ist die Abwägung zu treffen, einerseits Daten nicht unnötig lange zu behalten, um immer Muster eventuell doch noch erkennen zu können, anderseits Daten so lange zu speichern, um eine effektive Betrugserkennung nicht zu behindern.

Interessanter Gesichtspunkt ist dabei die Tatsache, dass die Identifizierung einer betroffenen Person nur bei konkretem Verdacht überhaupt notwendig ist, was nur einen geringen Prozentsatz der betroffenen Personen betrifft. Von überwiegendem Interesse ist die Profilbildung eines gewünschten, nicht-kriminellen Kunden und scharf abgegrenzt davon die Profilbildung eines potentiellen Betrügers. Die konkrete Person rückt damit völlig in den Hintergrund. Bislang haben sich übliche Speicherfristen, wie sie etwa für die Buchhaltung in § 132 Bundesabgabenordung mit 7 Jahren, bei der Geldwäsche mit 5 Jahren, oder einer zivilrechtlichen Verjährungsfrist von 3 Jahren, üblich sind, als durchaus ausreichend erwiesen.

8.2. Rechtsgrundlage für die Verarbeitung

Hinsichtlich der Rechtmäßigkeit der Verarbeitung bietet sich im Rahmen der Betrugsbekämpfung, und damit auch und gerade bei der financial crime prevention die Rechtsgrundlage der überwiegend berechtigten Interessen[23] an.[24] ErwGr 47 DSGVO vorletzter Satz sieht durch den Verordnungsgeber bereits die Möglichkeit vor, sich bei der Prüfung der Rechtsgrundlage der Verarbeitung auf ein berechtigtes Interesse zu stützen.[25] Die Verarbeitung personenbezogener Daten im für die Verhinderung von Betrug unbedingt erforderlichen Umfang stellt ein berechtigtes Interesse des jeweiligen Verantwortlichen dar und stellt damit in der Wahl der Datenquantität eine Schranke dar.

Dabei ist zu berücksichtigen, dass financial crime prevention nicht nur dem Finanzdienstleister dient, sondern auch der Betroffene vor finanziellem Schaden oder Identitätsdiebstahl geschützt wird. Eine gestohlene Identität ist für den Betroffenen eine direkte Beeinträchtigung seiner finanziellen Interessen und eine proaktive Verhinderung durch den Finanzdienstleister, dass dieser Diebstahl ins Leere führt. Gerade im Online-Geschäft und im Zahlungsverkehr wird der Betroffene eine Verwendung seiner Daten zur Verhinderung von Betrug erwarten können, bzw. ist er durch seine Teilnahme am Geschäftsverkehr bereits daran gewöhnt. Im Rahmen der Interessenabwägung kann daher davon ausgegangen werden, dass eine Einwilligung des Kunden in die Datenverwendung nicht notwendig ist.

---

21 Art 5 Abs 1 lit e DSGVO.

22 Zum Rechtfertigungsdruck: Frenzel, in: Paal/Pauly (Hrsg), Datenschutzgrundverordnung, Art 5 Z 43.

23 Art 6 Abs 1 lit f DSGVO.

24 Europäischer Datenschutzausschuss, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, S 14 unter Verweis auf dieselbe Meinung der damaligen Art. 29 Gruppe Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, WP 217, S 17.

25 Siehe dazu Plath, in Plath (Hrsg), BDSG DSGVO, Art 6 Z 21.

Unabhängig davon ist zur Erfüllung der Informationspflichten[26] der Betroffene an geeigneter Stelle über die Datenverwendung zu informieren. Im Online Bereich gilt dies nicht nur für Kunden, die den KYC-Prozess durchlaufen, sondern auch für Interessenten, welche sich erst im Vorfeld zum KYC befinden.

8.3. Personenbezug: wie weit geht eine «Distanzierung»?

ErwGr 30 der DSGVO beschreibt treffsicher den Sachverhalt, der bei der Datenlage hinsichtlich Kunden bereits erläutert wurde[27]: «Natürlichen Personen werden unter Umständen Online-Kennungen wie IP-Adressen und Cookie-Kennungen, die sein Gerät oder Software-Anwendungen und -Tools oder Protokolle liefern, oder sonstige Kennungen wie Funkfrequenzkennzeichnungen zugeordnet. Dies kann Spuren hinterlassen, die insbesondere in Kombination mit eindeutigen Kennungen und anderen beim Server eingehenden Informationen dazu benutzt werden können, um Profile der natürlichen Personen zu erstellen und sie zu identifizieren.» Damit ist gerade die Profilerstellung, hier zum Zweck der financial crime prevention, unter Heranziehung von Metadaten zweifelsohne im Online-Bereich erfasst.[28] Auch wenn einem Analysten die natürliche Person dahinter egal ist, besteht am Vorliegen eines datenschutzrechtlichen Personenbezug kein Zweifel.[29]

Wie bereits erläutert, hat in den letzten Jahren ein zweifacher Wandel in der Datenverwendung bei der financial crime prevention stattgefunden; einerseits vom direkten Personenbezug hin zum indirekten Personenbezug, andererseits von einem Datensatz mit nur wenigen Daten, hin zum exponentiellen Anstieg der Datenquantität mit einem Fokus nicht auf eine einzelne Person und sondern der Erkennung von Verhaltensmustern von Kriminellen schlechthin.

9. Zusammenfassung und Ausblick

Ungeachtet der rasanten technischen Entwicklung und der differenzierten Herangehensweise aus rechtlicher Sicht, die immer mehr auf einen risikobasierten Ansatz Bezug nimmt, ist ein Lösungsansatz der beiden Seiten gerecht wird, immer möglich. Kern dessen ist der iterative Ansatz in der Diskussion, der die Anforderungen des financial crime und des Datenschutzes vereint.

10. Literatur

Awad El-Sayed Ahmed, Ahmed & Traore, Issa, (11. 11 2014), Worldwide Patentnr. WO2004097601A1.

Bonstedt, Jan, Vom Personenbezug zum Gerätebezug – KI und Datenschutz. In: Die Macht der Daten und der Algorithmen. Regulierung von IT, Iot und KI, Oldenburger Verlag, Edewecht 2019.

Cao, Yinzhi, Li, Song & Wijmans, Erik (2017), (Cross-)Browser Fingerprinting via OS and Hardware Level Features. Proceedings of Network & Distributed System Security Symposium (NDSS). Von Yinzhi Cao: http://yinzhicao.org/TrackingFree/crossbrowsertracking_NDSS17.pdf, (Abgerufen am 13.12.2019).

Cox, Dennis, Handbook of Anti-Money-Laundering, John Wiley & Sons. New Jersey 2014.

Curry, Frederic (02. 04 2019). Financial Crime and Organizational Structure. (D. US, Interviewer) CFO Innovation. von https://www.cfoinnovation.com/risk-management/financial-crime-and-organizational-structure, (Abgerufen am 03.12.2019).

DeSantis, Matthew, Dougherty, Chad, McDowell, Mindi, US-Cert. von Understanding and Protecting Yourself Against Money Mule Schemes: https://www.us-cert.gov/sites/default/files/publications/money_mules.pdf, (Abgerufen am 03.12. 2019).

Ehmann/Selmayr, (Hrsg), Datenschutz-Grundverordnung, 1. Auflage, C.H. Beck, München 2017.

[26] Siehe Art 12ff DSGVO.

[27] Siehe Pkt 7.

[28] Siehe Jahnel, Dietmar/Bergauer, Christian, Teilkommentar zur DS-GVO, Art 4 Z 1 Rz 7.

[29] Siehe beispielhaft zur Diskussion des relativen/absoluten Personenbegriffs: Gola, in: Gola, Peter (Hrsg.), Datenschutz-Grundverordnung, Art 4 Rz 5 15ff.

Gola, Peter (Hrsg), Datenschutz-Grundverordnung, 1. Auflage, C.H. Beck, München 2017.

Jahnel, Dietmar/Bergauer, Christian, DS-GVO Datenschutz-Grundverordnung, Kommentar zu den Art 2-nnn, 13-1, 30, 35-37-39, Jan Sramek Verlag, Wien 2018.

Janssen, Gerhard, Betrug. in: Achenbach, Hans/Ransiek, Andreas (Hrsg), Handbuch Wirtschaftsstrafrecht, 3.Auflage (S. 523–587), C.F. Müller GmbH, Karlsruhe 2012.

Kasneci, Gjerji (26. September 2017). «Bereits bekannte Betrugsmuster werden durch die Anonymität im Netz vereinfacht.». (Bankingclub, Interviewer), https://www.bankingclub.de/news/fraudmanagement/bereits-bekannte-betrugsmuster-werden-durch-die-anonymitaet-im-netz-vereinfacht/ (Abgerufen am 04.12.2019).

McKinsey & Company. Global Payments Report 2019: Amid sustained growth, accelerating challenges demand bold actions. McKinsey & Company (2019) https://www.mckinsey.com/~/media/McKinsey/Industries/Financial%20Services/Our%20Insights/Tracking%20the%20sources%20of%20robust%20payments%20growth%20McKinsey%20Global%20Payments%20Map/McK-2019-Global-Payments-Report.ashx, (Abgerufen am 04.12.2019).

Norton by Symantec. (2019). Privacy, https://us.norton.com/internetsecurity-privacy-what-is-a-vpn.html (Abgerufen am 03. 12 2019).

Oracle (2019). What is big data?, https://www.oracle.com/big-data/guide/what-is-big-data.html (Abgerufen am 04.12. 2019).

Paal, Boris/Pauly, Daniel (HRSG), Datenschutz-Grundverordnung, 1. Auflage, C.H. Beck, München 2017.

Plath, Kai-Uwe (Hrsg), BDSG DSGVO, Kommentar zum BDSG und zur DSGVO sowie den Datenschutzbestimmungen des TMG und TKG, 2. Auflage, Otto Schmidt, Köln 2016.

Pritchard, Justin (09. 08 2019). Brick and Mortar Bank Branches, https://www.thebalance.com/brick-and-mortar-what-does-it-mean-315467, (Abgerufen am 03.12.2019).

Sudjianto, Agus, Nair, Sheela, Yuan, Ming., Zhang, Aijun, Kern, Daniel & Cela-Díaz, Fernando, Statistical Methods for Fighting Financial Crimes. Technometrics, 2017, S 5–19.

The Tor Project Inc (2019). About Tor: Overview: https://2019.www.torproject.org/about/overview.html.en, (Abgerufen am 03.12.2019).

The United States Department of Justice (07. 02 2017). What are Identity Theft and Identity Fraud, The United States Department of Justice: https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud, (Abgerufen am 1.12.2019).

Wex Inc, (27. 07 2017) Tokenization 101: Understanding the Basics: https://www.wexinc.com/insights/blog/corporate-payments-edge/credit-card-tokenization-basics/, (Abgerufen am 04.12.2019).