STIEGLER LEGAL

Smartphone-Fintech

Welche Rechtshürden müssen Banken bei der Erstellung und Verwendung von Mobile-Apps nehmen?

RA Frank Stiegler / Stiegler Legal

22. September 2016, ADG Forum IT-Sicherheit 2016, Schloss Montabaur

Der Hype ist deutlich.

„Die Volksbanken suchen die Super-App“
(FAZ, 08.03.2016)

Auch mit eigener Kontowechsel-App
(IT Finanzmagazin, 23.02.2016)

Mehr Begeisterung geht nicht: Detail aus dem Fintech Headquarter.

Artikel in der Frankfurter Rundschau vom 6. September 2016

Die Rechtshürden sind vielfältig.

Quelle: Pixabay-User hodihu: https://pixabay.com/de/perlen-bunt-makro-viele-farben-209341/

Apps spiegeln das Geschäft.

Quelle: Pixabay-User Markus_Christ: https://pixabay.com/de/skyline-rotterdam-architektur-1601187/

Quelle: Pixabay-User Comfreak:
https://pixabay.com/de/arbeiten-workaholic-schriftsteller-1627703/

Quelle: Pixabay-User mermyhh:
https://pixabay.com/de/deutsche-bank-frankfurt-bankgeb%C3%A4ude-456939/

Quelle: Pixabay-User Unsplash:
https://pixabay.com/de/u-bahn-zug-bahnhof-transport-stadt-1209556/

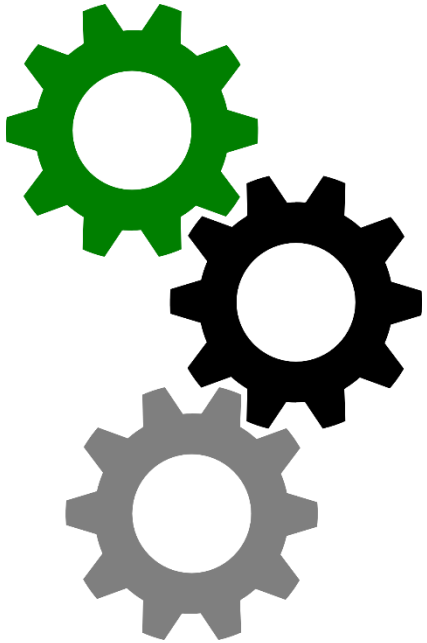
Quelle: Pixabay-User niekverlaan:
https://pixabay.com/de/telefon-handy-anrufen-erreichbar-586266/

App-Erstellung

Aufsicht

Quelle: Pixabay-User careyne:
https://pixabay.com/de/polizei-nachtsicht-menschen-495074/

API-Betreiber



Quelle: Pixabay-User Clker-Free-Vector-Images:
https://pixabay.com/de/zahnr%C3%A4der-gep%C3%A4cktr%C3%A4ger-ritzel-grau-306402/

Wettbewerber

Quelle: Pixabay-User morzaszum:
https://pixabay.com/de/stelle-l%C3%A4uft-start-la-stadion-862274/

Betroffene

Quelle: Pixabay-User Peggy Marco:
https://pixabay.com/de/maske-halloween-t%C3%BCte-kopf-1027226/

App-Betrieb

Weitere App-Spezifika (Bsp.)

- Datenschutz (BDSG → DSGVO + ABDSG):
  - Grundregeln: z. B. Datensparsamkeit, Verbot mit Erlaubnisvorbehalt
  - Hinweise, Interessenabwägung
  - ADV (Auftrags(daten)verarbeitung)
- Datensicherheit (v. a. PSD2, RTS, MaSI, PCI-DSS)
  - Inhalte von PSD2 mit Bezug zu Mobile-Apps auch für Fintechs
  - Umsetzung in nationales Recht: wann und wie?
  - XS2A: Problem für Banken, Zahlungsdiensteanbieter und Nutzer?
- Telemedienrecht (TMG):
  - Angabenpflichten (z. B. Impressum, Werbung, Preise, Risiken)
  - Haftung für eigenen/fremden Content
  - technische Sicherheit (explizit seit ITSG)
- Blockchain-Einsatz ○○○○

Yeah but no but yeah but no but yeah but...

Quelle: Pixabay-User aitoff: https://pixabay.com/de/polizei-lego-polizist-gesetz-1058422/

Quelle: Pixabay-User altoff: https://pixabay.com/de/lego-stormtrooper-star-wars-kraft-631850/

Allgemeine Rechtshürden

- Bankenaufsicht, SEPA-Bedingungen, Eigenkapitalrichtlinie (Basel III, MaRisk), …
- KWG, WpHG, GWG, Terrorfinanzierung, …
- Anzuwendendes Recht (v. a. bei Verbrauchern, Rom I)
- Urheber-/Persönlichkeitsrecht (UrhG, KUrhG), Rechte an Content (z. B. Stock Images)
- Markenrecht (MarkenG), z. B. bei Logonutzung
- Angaben-/Archivierungspflichten (z. B. § 34 WpHG)
- nicht-App-spezifischer Wettbewerb (UWG)
- Bitcoin

STIEGLER LEGAL

Vertrag mit Entwickler (Auszüge)

Definition des Auftrages

- vordefiniert und/oder agile Entwicklung?
- Dienst- oder Werkvertrag? → Ergebnis oder Bemühen geschuldet? Wer hat „den Hut auf“?
- Vorabprüfung der KO-Kriterien (z. B. verwendete Software, Lizenzen von Drittanbietern z. B. von APIs, technische Hürden)!
- Dokumentation Teil der Leistungen?
- Abnahmeszenario/-fiktion

Übertragung von Nutzungsrechten

- „Urheberrechte“ (!= Copyright): Urheberpersönlichkeitsrechte + Verwertungsrechte (übertragbar: **Nutzungsrechte**).
- Urheberpersönlichkeitsrechte: Verzicht (begrenzt ausreichend) möglich, ArbN übertragen Rechte auf ArbG (§ 69b UrhG).
- Problemkreis **Open-Source-Software** wg. Bindung an GPL & Co. → „Infektion“ von Software
- Achtung bei Subunternehmern des Entwicklers

Absicherung gegen (Sach- und Vermögens-)Schäden

Auftragsdatenverarbeitungsverhältnis (ADV)? § 11 BDSG → Art. 28 DSGVO

STIEGLER LEGAL

Die App im App-Store

Nutzungsbedingungen des Plattformbetreibers

- Google Play: https://play.google.com/intl/de_de/about/play-terms.html
- Apple App-Store: http://www.apple.com/legal/internet-services/itunes/de/terms.html

Authentizität des App-Anbieters im App-Store (u. a. wegen § 13 Abs. 7 TMG):

- **Authentizität des Anbieters** im App-Store: bei Google über Google-Konto, bei Apple über Apple-ID (jeweils verschlüsselt), Anmeldung bei Samsung Apps läuft noch unverschlüsselt. → ausreichend?

3-Personen-Verhältnis (mindestens): App-Store-Betreiber, App-Anbieter, Nutzer

- **Vertragspartner**? → Google Play-Nutzungsbedingungen: Direct Sale (Google), Agency Sale (Vertretung), App Sale (App-Anbieter)

Hinweis auf Nutzungsbedingungen, sonst Rechtsmangel (§§ 433 Abs. 1 S. 2, 435 BGB)

Datenschutzhinweise im App-Store: „geteilte Datenschutzverantwortlichkeit“?

STIEGLER LEGAL

Verhältnis zum Nutzer

Welches Recht ist anwendbar?

→ ROM I: grds. wählbar, aber bei Verbrauchergeschäften nach Art. 6 Abs. 1 grds. Recht des Landes, in dem der Verbraucher seinen gewöhnlichen Aufenthaltsort hat. Außerdem Verbraucherschutzrechte zwingend (Art. 6 Abs. 2).

App-Nutzungsbedingungen müssen (aktiv) akzeptiert werden.
Nachgeschobener Hinweis reicht nicht.

Datenschutzhinweise (§ 13 TMG → Art. 12 Abs. 1 DSGVO), neu z. B.:

- Nennung der berechtigten Interessen
- Zeitpunkt des Hinweises: bei Erhebung (nicht mehr „zu Beginn des Nutzungsvorgangs“)
- keine Rückwirkung des Widerrufs

Problem bei XS2A: ggf. Verstoß gegen Nutzungsbedingungen der Bank

→ Verpflichtung, Login-Daten zu Online-Konto nicht weiterzugeben (was man bei XS2A aber muss)

STIEGLER LEGAL

Fintech: wenn App-Anbieter != Bank

Brauchen alle Fintechs nach PSD2 eine Zulassung durch die EBA?

- Nein, das ist abhängig davon, ob sie **Zahlungsdienste erbringen** wollen
  (dann Zulassung als Zahlungsinstitut iSv. Art. 4 Nr. 4 PSD2 erforderlich (Art. 11 Abs. 1 PDS2).
- Zulassung wird auf Antrag erteilt, wenn u. a. folgende **Angaben/Nachweise** beigefügt sind (Art. 5 Abs. 1 PSD2) und eine „**positive Gesamtbewertung**“ erlangt wird:
  - Geschäftsmodell und Geschäftsfortführung im Krisenfall
  - Sicherheitskonzept insbes. für Geldbeträge
  - Unternehmenssteuerung
  - Prozess zur Überwachung/Handhabung von Sicherheitsvorfällen und einschlägigen Kundenbeschwerden
  - Verfahren zur Handhabung sensibler Zahlungsdaten
- Berufshaftpflicht- oder ähnliche Versicherung erforderlich (Art. 5 Abs. 2 PSD2)

starke Authentifizierung erforderlich (Art. 4 Nr. 30 PSD2)
→ 2-Faktor-Authentifizierung, bisherige TAN-/iTAN-Verfahren nicht PSD2-konform.

Sichere Kommunikation (Weitergabekontrolle nach Anlage zu § 9 BDSG): Kryptographie

STIEGLER LEGAL

Zahlungsauslöse-/Kontoinformations-DA

XS2A bringt „**diskriminierungsfreiem Zugang**“ zu Kontodaten (Art. 66 Abs. 1 PSD2)
→ ZAD (Art. 4 Nr. 15 PSD2) und KID (Art. 4 Nr. 16 PSD2), bisher beide Arten von Dienstanbietern erlaubnisfrei nach § 1 Abs. 10 Nr. 9 ZAG

Pflichten (Auszug) des ZAD in Art. 66 PSD2 Abs. 3 geregelt, v. a.:

- **darf kein Geld halten** (lit. a) und keine sensiblen Zahlungsdaten speichern (lit. e)
- muss sicherstellen, dass „Daten des Nutzers“ (lit. b, c) nur dem Nutzer und dem Emittenten zugänglich sind
- darf vom Nutzer **nur die erforderlichen Daten** fordern (lit. f)
- **Zweckbindung** (lit. g)

Pflichten (Auszug) des KID (Art. 67 Abs. 2 PSD2): selbe Prinzipien wie der ZAD, zusätzlich

- darf seine Leistungen **nur mit ausdrücklicher Zustimmung** des Nutzers erbringen (lit. a)
- muss sich bei jedem Kommunikationsvorgang identifizieren und sicher kommunizieren (lit. c)
- darf **keine sensiblen Zahlungsdaten** anfordern (lit. e)

STIEGLER LEGAL

Stand von PSD2 in Deutschland

Umsetzung in nationales Recht bis 13.01.2018 gefordert.
Bislang nur eine Stellungnahme vom Bitkom vom 24. Juni 2016 dazu gefunden.

Konsultationspapier der EBA vom 12. August 2016 zur starken Kundenauthentifizierung und Kommunikationsstandards zwischen Zahlungsdienstleistern und Dritten (ZAD/KID):

- enthält kaum technische Standards
- verweist u. a. auf ISO 20022 und sonstigen Kommunikationsstandards
- Konsultationsphase läuft bis 12. Oktober 2016.

Finaler RTS-Entwurf bis zum 12. Januar 2017 veröffentlicht, anwendbar aber erst 18 Monate nach seiner Annahme durch die EU-Kommission (**frühestens Oktober 2018**).

Finale RTS wohl in Form einer **delegierten Verordnung (unmittelbar anwendbar).**

STIEGLER LEGAL

ITSG/BSIG → Kritische Infrastrukturen

§ 8b Abs. (3) BSIG: Betreiber müssen BSI **binnen 6 Monaten** nach Inkrafttreten einer einschlägigen BSI-KritisV (erste VO vom 4. August 2016, Finanzsektor bislang nicht geregelt) eine **Kontaktstelle für die Kommunikationsstrukturen** benennen, vor allem für:

Krisenfrüh**erkennung**	Krisen**reaktion**	Krisen**bewältigung**

Abs. (4): Pflicht, **erhebliche Störungen** der **Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit** der IT-Systeme, Komponenten oder Prozesse, **die zu** einem Ausfall oder **einer Beeinträchtigung der Funktionsfähigkeit** der von ihnen betriebenen **Kritischen Infrastrukturen** führen **können oder geführt haben, unverzüglich zu melden.**

STIEGLER LEGAL

Die DSGVO kommt (diesmal wirklich)

DSGVO trat am 25. Mai 2016 in Kraft, **wird wirksam am 25. Mai 2018**.
Übersicht zum Verfahrensgang auf CR online

Am 5. August 2016 wurde ein **erster Referentenentwurf** zur Anpassung des BDSG („BDSG-Rumpfgesetz“) veröffentlicht.

Neu: DSGVO ist anwendbar, wann immer Daten von in der EU befindlichen Personen betroffen sind, **auch bei Auftragsverarbeitern mit Sitz außerhalb der EU** (ErwGr 24 S. 2).

Ziel: **EU-weite Vereinheitlichung** des Datenschutzes. Raum für nationale Besonderheiten an bestimmten Stellen gelassen, z. B. bei Arbeitnehmerdatenschutz, Regeln zur Bestellpflicht von DSB.

STIEGLER LEGAL

DSGVO: Änderungen (Auszug)

„Identifizierbarkeit“ ersetzt die bisherige **Personenbeziehbarkeit** (Art. 4 Abs. 1):

„als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels **Zuordnung zu einer Kennung** wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer **Online-Kennung** oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;“ Erwägungsgrund: „Um festzustellen, ob eine […] Person identifizierbar ist, **sollten alle Mittel berücksichtigt werden, die […] nach allgemeinem Ermessen wahrscheinlich genutzt werden** […]“

Hierdurch **entfällt die „Stufe“ der Pseudonymisierung**. Bislang wird in vielen Bereichen (z. B. im Online-Marketing) vieles über Einwilligung des Betroffenen gelöst, was bei pseudonymen Cookies nicht nötig war. Zukünftig zählen auch pseudonyme Daten als personenbezogen.

STIEGLER LEGAL

DSGVO: Änderungen (Auszug)

Einwilligung wird wegen steigenden Informationspflichten schwieriger, Interessenabwägung mit „vernünftiger Erwartung“ Regelfall:

- Einwilligungen werden wg. höheren Anforderungen schwerer zu bekommen, aber praktisch auch weniger wichtig sein.
- Deutlich bedeutsamer werden Angabenpflichten und die **Abwägung von „schutzwürdigen Interesse“ und Betroffenenrechten** sein („**vernünftige Erwartung**“ nach ErwGr 47).

DSB-Regelung ist nach der DSGVO nicht so streng wie das bisherige BDSG, aber der aktuelle Änderungsentwurf liest sich, als wolle der deutsche Gesetzgeber die bisherige Regelung beibehalten.

TOM „Zutritts-, Zugangs-, Zugriffs-, Weitergabekontrolle“ werden zu allgemeiner **Pflicht zu Vertraulichkeit und Integrität**, ohne offensichtliche inhaltliche Veränderung.

STIEGLER LEGAL

DSGVO: Änderungen (Auszug)

ADV (§ 11 BDSG) → AV (Art. 28 DSGVO): Das **Auftragsverhältnis ist nicht mehr zwingend weisungsgebunden** (war realitätsfern). „Funktionsübertragung“ (Abgrenzung zur ADV) faktisch überflüssig. Der AV wird stärker in die Pflicht genommen, kann sich nicht mehr auf Weisungsgebundenheit berufen.

Recht auf Vergessenwerden (Art. 17 Abs. 1 lit. f DSGVO): „Löschen“ meint die Unbenutzbarkeit für den gewöhnlichen Gebrauch (realitätsnäher).

Profiling (enthält Scoring und Screening): **Angaben zu Algorithmuslogik** erforderlich. Widerspruchsrechte nach Art. 21 DSGVO.

Vorabkontrolle → **Folgenabschätzung** (Art. 35 DSGVO)

STIEGLER LEGAL

Kontowechsel-App: UWG-Verstoß?

§ 3 Abs. 1 UWG: „Unlautere geschäftliche Handlungen sind unzulässig."

§ 4 UWG: „**Unlauter handelt, wer** […] [4.] **Mitbewerber gezielt behindert.**"

Sind **Kontowechsel-Apps eine gezielte Wettbewerbsbehinderung** nach § 4 Nr. 4 UWG?

OLG München, Beschluss v. 22.06.2005, Az. 6 U 4627/04: Kaufland-Center Dessau, Klage **gegen Media Markt** wegen großer roter Pfeile mit Aufdruck "Da lang" auf Fußboden und an Balustrade direkt vor Konkurrenzgeschäftslokal → **gezielte Behinderung** (+), kein Urteil.

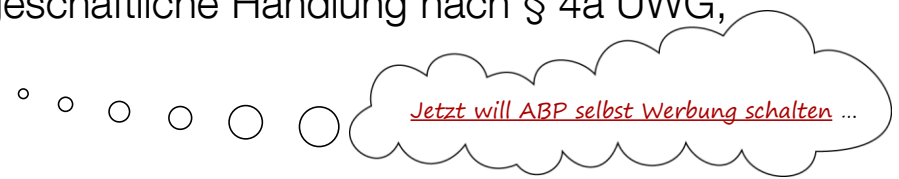
OLG Stuttgart, Urteil v. 2. Juli 2015, Az.: 2 U 148/14 (damals war die gezielte Behinderung noch in § 4 Nr. 10 UWG geregelt): **Klage gegen Drogeriekette**, die Rabattgutscheine von Konkurrenten annahm, **abgewiesen**. Auch Nennung einzelner Wettbewerber in Ordnung.

STIEGLER LEGAL

Kontowechsel-App: UWG-Verstoß?

§ 4a Abs. 1 UWG: „Unlauter handelt, wer eine **aggressive geschäftliche Handlung** vornimmt, die geeignet ist, den **Verbraucher oder sonstigen Marktteilnehmer** zu einer geschäftlichen **Entscheidung zu veranlassen, die dieser andernfalls nicht getroffen hätte**. […], wenn sie **im konkreten Fall unter Berücksichtigung aller Umstände** geeignet ist, die **Entscheidungsfreiheit** des Verbrauchers oder sonstigen Marktteilnehmers **erheblich** zu beeinträchtigen […]“

Urteil des OLG Köln v. 24.06.2016, Az. 6 U 149/15: **Axel Springer ./. Adblock Plus**: „wie Abreißen von Werbeplakaten“. Gericht bejahte das Wettbewerbsverhältnis bejaht, hielt das Prinzip von Adblocking nicht für aggressive geschäftliche Handlung nach § 4a UWG, das **Whitelisting-Bezahlmodell** das schon.



Fazit

1. Verträge mit externen App-Erstellern: Definition der App, Nutzungsrechte, datenschutzgerechte Einbindung essenziell
2. In Zukunft kritisch: Hinweise an App-Nutzer, sichere Kommunikation (2-Faktor-Authentifizierung), Dokumentation/Protokollierung der Prozesse
3. PSD2 bringt u. a. durch XS2A Bewegung, muss noch umgesetzt werden. RTS wohl als delegierter Rechtsakt.
4. DSGVO wird am 25.05.2018 wirksam, Änderung des BDSG läuft.
5. Apps unterliegen zusätzlich den üblichen Regeln geschäftlichen Handelns.

Quelle: Pixabay-User RemazteredStudio: https://pixabay.com/de/sport-laufband-strecke-f%C3%BChrte-1201014/

Viel Erfolg!

RA Frank Stiegler
Martin-May-Straße 10
60594 Frankfurt

Fon: +49 69 96866084
E-Mail: stiegler@stiegler-legal.com

Bildquellenangaben / Image Sources

- S. 3 Bunte Perlen, Pixabay-User **hodihu**: https://pixabay.com/de/perlen-bunt-makro-viele-farben-209341/
- S. 4 Rotterdam-Skyline, Pixabay-User **Markus_Christ**: https://pixabay.com/de/skyline-rotterdam-architektur-1601187/
- Ss. 5, 9, Programmierer auf Bank, Pixabay-User **Comfreak**: https://pixabay.com/de/arbeiten-workaholic-schriftsteller-162
- Ss. 5, 12, 13 Deutsche Bank-Hochaus, Pixabay-User **mermyhh**: https://pixabay.com/de/deutsche-bank-frankfurt-bankgebäude-45
- Ss. 5, 10 Bahnsteig, Pixabay-User **Unsplash**: https://pixabay.com/de/u-bahn-zug-bahnhof-transport-stadt-120
- Ss. 5, 11 Smartphone in Hand, Pixabay-User **niekverlaan**: https://pixabay.com/de/telefon-handy-anrufen-erreichbar-58626
- Ss. 6, 15 Polizist, Pixabay-User **careyne** https://pixabay.com/de/polizei-nachtsicht-menschen-495074/
- Ss. 6, 12 , 13Zahnräder, Pixabay-User **Clker-Free-Vector-Images**: https://pixabay.com/de/zahnräder-gepäckträger-ritzel-grau-
- Ss. 6, 20, 21 Wettlauf, Pixabay-User **morzaszum**: https://pixabay.com/de/stelle-läuft-start-la-stadion-86227
- Ss. 6, 16 , 17, 18, 19Figur mit Kopf-Pappkiste, Pixabay-User **Peggy Marco**: https://pixabay.com/de/maske-halloween-t%C3%BCte-kopf-1027226/
- Ss. 7, 14 Lego-Polizist, Pixabay-User **aitoff**: https://pixabay.com/de/polizei-lego-polizist-gesetz-1058422/
- Ss. 7, 8 Gedankenblase, Pixabay-User **Clker-Free-Vector-Images**: https://pixabay.com/de/wolken-wei%C3%9F-symbol-anmelden-denken-34428/
- S. 8 Lego-Storm Trooper, Pixabay-User **aitoff**: https://pixabay.com/de/lego-stormtrooper-star-wars-kraft-631850/
- S. 22 Zielgerade, Pixabay-User **RemazteredStudio**: https://pixabay.com/de/sport-laufband-tor-strecke-f%C3%A4hrte-1201014/

Your images make this presentation so much nicer! Thank you!