MARKTWÄCHTER
DIGITALE WELT

verbraucherzentrale

E-PAYMENT – WIE SICHER SIND UNSERE DATEN BEIM BEZAHLEN IM NETZ?

Eine Untersuchung der Verbraucherzentralen – November 2017

INHALT

ABBILDUNGEN UND TABELLEN 5

ZUSAMMENFASSUNG 7

1. ZIELSETZUNG & METHODIK 9
   Zielsetzung 9
   Methodik 11

2. DATENSICHERHEIT 16
   Wie sicher ist die Verschlüsselung der Kommunikation? 17
   Wie sicher ist die Anmeldung beim Bezahldienstleister? 18
   Wie erfolgt die technische Absicherung der Benutzersitzung? 19
   Wie ist der effektive Schutz gegen Angriffe im Browser gestaltet? 19
   Welche weiteren Schwachstellen wurden gefunden? 20
   Fazit: Hohes Sicherheitsniveau wird gewährleistet 20

3. DATENSPARSAMKEIT 21
   Welche Daten werden während Registrierung und Bezahlprozess erhoben? 21
   Welche Tracking-Dienste verwenden die Bezahldienstleister? 24
   Fazit: Nicht jeder Bezahldienstleister folgt der Datensparsamkeit 24

4. TRANSPARENZ IM UMGANG MIT VERBRAUCHERDATEN 26
   Welche rechtlichen Anforderungen gelten für Datenschutzerklärungen? 26
   Wie wird in den Datenschutzerklärungen informiert? 27
   Zu welchen Zwecken werden die Verbraucherdaten verwendet? 28
   Wie verständlich sind Datenschutzerklärungen? 29
   Fazit: Datenschutzerklärungen lassen Interpretationsspielraum und sind schwer verständlich 30

5. RECHT AUF AUSKUNFT 32
   Was beinhaltet das Recht auf Auskunft? 32
   Wie reagieren Bezahldienstleister auf das Auskunftsverlangen? 33
   Wie wird in den Auskunftsschreiben informiert? 34
   Wie verständlich sind die Auskunftsschreiben? 35
   Fazit: Der Umgang mit dem Recht auf Auskunft ist verbesserungswürdig 36

6. VERBRAUCHERERWARTUNG AN DEN DATENSCHUTZ 37
   Welche Daten würden Verbraucher weitergeben? 37
   In welchem Umfang wollen Verbraucher informiert werden? 38
   In welcher Form wollen Verbraucher informiert werden? 40
   Kennen und wünschen Verbraucher das Recht auf Auskunft? 42
   Fazit: Auftrag der Verbraucher – kurze, verständliche Datenschutzerklärungen mit Entscheidungsmöglichkeit 43

7. SCHLUSSFOLGERUNGEN 44

8. GLOSSAR 47

9. QUELLENVERZEICHNIS 50

ABBILDUNGEN UND TABELLEN

1 Zielsetzung, Fragestellung und Methodik 12

2 Man-in-the-Middle-Angriff 16

3 Schematische Darstellung eines SSl-Stripping-Angriffs 18

4 Anzahl übermittelter Nutzerdaten bei Registrierung und Bezahlung 23

5 Eingesetzte Tracking-Dienste auf den Seiten der Bezahldienstleister 25

6 Zweck der Datenverwendung 28

7 Formale Texteigenschaften der Datenschutzerklärungen 30

8 Beispielsätze aus den untersuchten Datenschutzerklärungen 31

9 Überblick des Auskunftsprozesses 33

10 Angaben in den Auskunftsschreiben 35

11 Formale Texteigenschaften der Auskunftsschreiben 36

12 Zitate zur Weitergabe persönlicher Daten bei freier Entscheidung 38

13 Bereitschaft zur Weitergabe von Daten an Bezahldienstleister 39

14 Anforderungen der Nutzer an den Umfang der Informationen 39

15 Präferierte Zeit der Nutzer zum Lesen der Informationen 40

16 Zitate zu Formaten zu Informationen der Datenpraxis 41

17 Eignung verschiedener Informationsformate aus Sicht der Verbraucher 41

18 Kenntnis des gesetzlichen Rechts auf Auskunft nach § 34 BDSG 42

19 Wunsch, Auskunft vom Bezahldienstleister zu erhalten 43

ZUSAMMENFASSUNG

Das Team des Marktwächters Digitale Welt der Verbraucherzentrale Brandenburg hat die sechs am Markt aktivsten Bezahldienstleister Amazon Pay, giropay, paydirekt, PayPal, Skrill und SOFORT Überweisung untersucht: Technische Sicherheitsmaßnahmen bei der Bezahlung im Web-Browser wurden in den Blick genommen und hinsichtlich möglicher Schwachstellen durchleuchtet. Zudem hinterfragten die Experten die Einhaltung des Prinzips der Datensparsamkeit und ermittelten, wie transparent und verständlich elektronische Bezahldienstleister über die Verwendung von Verbraucherdaten informieren. Ferner zeigen Auskunftsverlangen den Umgang der Dienstleister mit den Nutzern und deren Daten.

OFTMALS NICHT „DATENSPARSAM“, ABER HOHES SICHERHEITSNIVEAU

Das Sicherheitsniveau der untersuchten elektronischen Bezahldienstleister ist gemessen an allgemeinen Web-Anwendungen hoch. Die Verschlüsselung der Kommunikation zwischen dem Browser des Nutzers und dem Server des Dienstleisters wird auf Basis des durchgeführten Gutachtens als sicher eingeschätzt. Bei Phishing-Attacken gibt es jedoch keinen durchgängig wirksamen Schutz. Eine zusätzliche Sicherung über eine Content Security Policy haben Amazon Pay, paydirekt und PayPal implementiert.

Das Prinzip der Datensparsamkeit wird unterschiedlich eingehalten. Die Anzahl erhobener Nutzerdaten durch die Dienstleister bei Registrierung und Bezahlvorgang variiert zwischen vier und 13 Einzeldaten. Dienste ohne Registrierung, wie giropay und SOFORT Überweisung, erheben vergleichsweise wenige Daten. Auch die Anzahl übermittelter Daten zwischen Händler und Bezahldienstleister unterscheidet sich: Paydirekt und PayPal tauschen deutlich mehr Daten mit dem Händler. Amazon Pay hat zudem Zugriff auf das Amazon-Nutzerkonto. Ferner variieren die Anzahl eingebundener Tracking-Dienste, der Ort ihres Einsatzes, die Art der erhobenen Daten und die Weiterleitung durch die Tracking-Dienste deutlich zwischen den Bezahldienstleistern: Während paydirekt auf die Nutzung eines externen Dienstes setzt, bindet Skrill elf Dienste ein. Skrill verwendet vier seiner Tracking-Dienste auch nach dem Login – alle sind geeignet personenbeziehbare Daten zu erheben. Zwei dieser Dienste teilen Daten auch mit Dritten.

DATENSCHUTZERKLÄRUNGEN HÄUFIG UNKONKRET UND UNVERSTÄNDLICH

Bis auf den Anbieter Skrill informieren alle untersuchten Bezahldienstleister in den Datenschutzerklärungen im Rahmen der gesetzlichen Anforderungen. Das Ergebnis der Untersuchung zeigt: Angaben zur Art erhobener und weitergegebener personenbezogener Daten sowie den jeweiligen Empfängern werden nicht abschließend ausgeführt. Wendungen wie „zum Beispiel“, „möglicherweise“ und „unter anderem“ lassen erheblichen Interpretationsspielraum zu. Damit können Verbraucher[1] nicht klar erkennen, worauf sie sich bei Nutzung des Dienstes einlassen.

Die formale Verständlichkeit der untersuchten Datenschutzerklärungen bewegt sich zwischen unverständlich und schwer verständlich. So sind es insbesondere lange Sätze, Passivkonstruktionen und Füllwörter, die dem Leser die Verständlichkeit erschweren. Die Länge der Erklärungen und damit der zeitliche Leseaufwand für den Nutzer variiert: So benötigt ein Leser der Datenschutzerklärung von SOFORT Überweisung vier Minuten; im Fall von PayPal bedarf es 24 Minuten.

DISKREPANZ ZWISCHEN VERBRAUCHERMEINUNG UND REALITÄT

Die Ergebnisse zum Umfang, der Lesedauer und der Verständlichkeit der Datenschutzerklärungen zeigen: Die Realität geht teilweise deutlich an den Wünschen der Verbraucher vorbei. Laut repräsentativer Verbraucherbefragung im Rahmen vorliegender Untersuchung wünschen die Nutzer, nicht mehr als fünf Minuten Zeit damit zu verbringen, die Datenschutzerklärungen eines Bezahldienstleisters zu lesen. Auch dem benannten Wunsch nach einem kurzen, übersichtlichen und verständlichen – möglichst einseitigen – Format kommt kein Anbieter nach. Von den Nutzern angeregt wird ein

1 Die gewählte männliche Form bezieht sich immer zugleich auf weibliche und männliche Personen. Wir bitten um Verständnis für den weitgehenden Verzicht auf Doppelbezeichnungen zugunsten einer besseren Lesbarkeit.

Format mit aktiver Wahl bzw. Abwahl zu erhebender Einzeldaten.

Daten, welche die befragten Nutzer preiszugeben bereit sind, umfassen: Name, Geburtsdatum, Kontaktdaten und Bankverbindungsdaten. Nahezu jeder Fünfte äußert darüber hinaus, nur die zur Abwicklung einer Zahlung wirklich notwendigen Daten bzw. so wenig Daten wie möglich weitergeben zu wollen. Daten zur eigenen Kredithistorie, dem Nutzungsverhalten und dem Standort möchten die befragten Nutzer auf Nachfrage überwiegend nicht von sich preisgeben.

AUSKUNFTSVERFAHREN VERBESSERUNGSWÜRDIG

Auf das Auskunftsersuchen der Testkäufer im Rahmen der Untersuchung haben die Bezahldienstleister sehr unterschiedlich reagiert – ein verlässliches, einheitliches Verfahren scheint derzeit nicht etabliert: Eine sofortige Auskunft gaben paydirekt und SOFORT Überweisung. Eine standardisierte Kunden-E-Mail ohne Bezug zum Anliegen versandten Amazon Pay und PayPal. Gar keine Reaktion auf das erste Schreiben erfolgte bei den Anbietern giropay und Skrill.

Auch die Identitätsüberprüfung wurde unterschiedlich gehandhabt: PayPal verlangt die Übersendung eines Identitätsnachweises mit sichtbarer Identifikationsnummer des Personalausweises. SOFORT Überweisung kam der Bitte auf Auskunft nach Zusenden eines geschwärzten Identitätsnachweises nach. Skrill knüpft an die Erlangung der Auskunft ein Entgelt. Die Dauer bis zur Übermittlung der Auskunftsschreiben variierte zwischen zwei und 62 Tagen.

Die Ergebnisse der Befragung zeigen in diesem Zusammenhang: Nur gut ein Drittel der Befragten (35 Prozent) weiß derzeit von seinem Recht auf Auskunft. Dabei besteht bei der deutlichen Mehrheit der befragten Nutzer (84 Prozent) der Wunsch, vom genutzten elektronischen Bezahldienstleister eine Auskunft über die Erhebung und Verwendung persönlicher Daten zu erhalten.

1. ZIELSETZUNG & METHODIK

Die Untersuchung des Marktwächters Digitale Welt „E-Payment – Bezahlen im Internet“[2] verdeutlichte die Beliebtheit elektronischer Bezahldienstleister bei Online-Käufern. Gleichzeitig wurde das Dilemma offensichtlich, vor dem viele Verbraucher stehen: Einerseits wollen sie an den bequemen, schnellen und scheinbar kostenfreien Lösungen der Bezahldienstleister teilhaben. Andererseits geben sie ihr Einverständnis für etwas, das sie eigentlich nicht wollen – die Weiterverwendung ihrer Daten. Die zweite große Sorge der Verbraucher gilt der Sicherheit ihrer Daten und damit der Angst vor Missbrauch durch Kriminelle.

ZIELSETZUNG

Vor diesem Hintergrund widmet sich die vorliegende Untersuchung der beiden von Verbraucherseite benannten Problemfelder: **der Datensicherheit und -sparsamkeit sowie der Transparenz im Umgang mit Verbraucherdaten durch elektronische Bezahldienstleister. Weiterhin wird dargelegt, wie Verbraucher über die Verwendung ihrer Daten informiert werden wollen.**

Zur Abgrenzung des Untersuchungsgegenstandes wird auf die bestehende Definition elektronischer Bezahlverfahren[3] zurückgegriffen:

Elektronische Bezahlverfahren sind über elektronische Netzwerke abgewickelte Bezahlvorgänge als Gegenleistung für den Bezug von Gütern und Dienstleistungen, die eigens für die Abwicklung des Kaufes im Internet entwickelt wurden und nicht ausschließlich über mobile Endgeräte ausgelöst werden können.

Von den elf am Markt aktiven Anbietern elektronischer Bezahlverfahren[4] wurden **Amazon Pay**, **giropay**, **paydirekt**, **PayPal**, **Skrill** und **SOFORT Überweisung** in die Untersuchung einbezogen.

„No data – no retail“ – jede gewonnene Kundeninformation und jedes gemessene Verhaltensmuster liefert neue Ansatzpunkte, um personalisierte Produkte und Dienste anzubieten[5]. Diese Erkenntnis ist lange im Markt angekommen, das Sammeln von Verbraucherdaten gängige Praxis, die Anwendungen vielfältig.

Somit ist es der entscheidende Wettbewerbsvorteil für Händler und Dienstleister – sowohl im digitalen als auch im stationären Handel. Aus Verbraucherschutzsicht bleibt es in Zeiten von Big Data maßgeblich, dass jeder Einzelne sein Grundrecht auf informationelle Selbstbestimmung effektiv in Anspruch nehmen kann[6]. Die Realisierung der Selbstbestimmung ist in der Praxis von unterschiedlichen Voraussetzungen abhängig: Wie den Pflichten des Bezahldienstleisters, verantwortungsvoll mit den Nutzerdaten umzugehen und datenschutzrechtliche Vorgaben einzuhalten. Zum verantwortungsvollen Umgang mit Daten zählt auch die Gewährung der Sicherheit der Verbraucherdaten. Ebenso müssen die Einhaltung des Prinzips der Datensparsamkeit und die transparente Aufklärung über die Verwendung der Verbraucherdaten gesichert sein.

2 Vgl. Dautzenberg et al. (2017a): E-Payment – Bezahlen im Internet, Marktdynamik und Verbrauchersicht auf elektronische Bezahlverfahren im deutschen Internet-Handel, online verfügbar unter: http://www.marktwaechter.de/sites/default/files/downloads/untersuchungsbericht_marktwaechter_e-payment_pdf.pdf, Stand 07.08.2017.

3 Vgl. Dautzenberg et al. (2017a), S. 14.

4 Zur Ermittlung der angebotenen elektronischen Bezahlverfahren wurden im März 2017 die 100 umsatzstärksten Online-Händler aus dem Jahr 2015 sowie die 81 umsatzstärksten Content- und Serviceanbieter aus dem Jahr 2014 untersucht und insgesamt elf Anbieter identifiziert: Amazon Pay, barzahlen.de, giropay, Google Wallet, MasterPass, Neteller, paydirekt, PayPal, paysafecard, Skrill und SOFORT Überweisung. Die sechs ausgewählten Bezahldienstleister vereinen den höchsten Marktanteil auf sich. (vgl. Dautzenberg et al. (2017a), S. 24).

5 Vgl. Dapp (2015): Fintech reloaded – Die Bank als digitales Ökosystem, Deutsche Bank, online verfügbar unter: https://www.dbresearch.de/PROD/RPS_DE-PROD/PROD0000000000443890/Fintech_reloaded_%E2%80%93_Die_Bank_als_digitales_%C3%96kosyste.pdf, Stand 07.08.2017, S. 23.

6 Dieses Recht leitet sich aus Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG (sog. Volkszählungsurteil, BVerfG, Urteil vom 15. September 1983, 1 BvR 209/83) her und wird als das Recht jedes Einzelnen verstanden, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen. Es ist damit nicht explizit im Grundgesetz geregelt, sondern wurde vom Bundesverfassungsgericht aus dem allgemeinen Persönlichkeitsrecht entwickelt.

Dies gilt insbesondere, da es sich bei einem Großteil der bei einem Bezahlvorgang angegebenen Daten um personenbezogene Daten[7] handelt.

Datensicherheit

Der Grundsatz der Datensicherheit ist gemäß § 9 Bundesdatenschutzgesetz (BDSG) durch das Treffen technischer und organisatorischer Maßnahmen zu gewährleisten. Ziel der Maßnahmen ist die Wahrung der Verfügbarkeit, Unversehrtheit und Vertraulichkeit von Informationen. Dies erfolgt mittels Sicherheitsvorkehrungen bei der Anwendung von informationstechnischen Systemen, Komponenten und Prozessen. Die für die Datenverarbeitung Verantwortlichen sind dazu verpflichtet, Daten vor dem Zugriff durch unbefugte Dritte zu schützen.

Ziel der vorliegenden Studie ist es zu ermitteln, inwiefern elektronische Bezahldienstleister gängigen Datensicherheitsstandards genügen und Verbraucher bei der Nutzung elektronischer Bezahlverfahren sicher gehen können, dass ihre Daten vor Missbrauch durch Dritte geschützt sind.

Datensparsamkeit

Datensparsamkeit orientiert sich am Ziel, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten und zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren soweit dies nach dem Verwendungszweck möglich ist[8]. Damit eng verbunden ist der Grundsatz der Zweckbindung. Dieser besagt, dass jeder Verarbeitung von personenbezogenen Daten ein bestimmter Zweck zugrunde liegen muss. Dieser muss vor der Verarbeitung festgelegt worden sein. Datenspeicherungen auf Vorrat ohne einen bestimmten Zweck sind unzulässig. Demnach ist die Verarbeitung personenbezogener Daten stets an dem Ziel auszurichten, so wenige Daten wie möglich zu verarbeiten.

Ziel ist es zu eruieren, inwieweit die elektronischen Bezahldienstleister dem Prinzip der Datensparsamkeit nachkommen und ob sie über die Erbringung der Dienstleistung hinausgehend Daten von Verbrauchern erheben.

Transparenz im Umgang mit Verbraucherdaten

Das Recht auf informationelle Selbstbestimmung kann nur wirksam angewendet werden, wenn über die Datenverarbeitung transparent informiert wird. Hierzu stellt der Bezahldienstleister üblicherweise eine Datenschutzerklärung zur Verfügung. Diese kann in Teilen einwilligungsrelevante Tatbestände enthalten. In diese muss der Nutzer im Vorfeld der Dienstleistung zustimmen. Hierbei kann er derzeit vor einem Problem stehen: Eine Entscheidung des Verbrauchers gegen die Nutzung seiner Daten ist gleichbedeutend mit der Entscheidung gegen die Nutzung des Dienstes. Somit kann die Nutzung des Dienstes in der Praxis zwingend an die Herausgabe weiterer Daten gekoppelt sein, die für die Vertragsdurchführung nicht immer erforderlich sind. Wirkliche Entscheidungsfreiheit besteht nur, wenn der Nutzer Einfluss darauf nehmen kann, welche Daten erhoben, verarbeitet und genutzt werden. Hierfür muss er Informationen erhalten, die ihm konkret verdeutlichen, wer wann was mit seinen Daten macht.

Ziel ist es zu erarbeiten, ob und wie Verbraucher über die Erhebung, Verarbeitung und Nutzung ihrer Daten informiert werden.

Recht auf Auskunft

Dem Verbraucher[9] stehen nach dem BDSG gegenüber dem datenverarbeitenden Unternehmen unterschiedliche Rechte zu[10]. Von Bedeutung ist hier insbesondere das Recht des Verbrauchers auf Auskunft. Das Unternehmen muss ihn über die zu seiner Person gespeicherten Daten, die zu Empfängern weitergeleiteten Daten sowie zum Zweck der Speicherung informieren[11]. Darüber hinaus kann der Verbraucher bei unrichtigen

7 Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (vgl. § 3 Abs. 1 BDSG). Eine Person wird dabei als bestimmbar angesehen, wenn sie direkt oder indirekt identifiziert werden kann (vgl. Art. 2 Buchst. A Richtlinie 95/46/EG).

8 Vgl. § 3a BDSG.

9 Das BDSG spricht von Betroffenen. Betroffene im Sinne des § 3 Abs. 1 BDSG sind natürliche Personen. Hierunter fallen unter anderem auch Verbraucher im Sinne des § 13 BGB. Zur vereinfachten Verständlichkeit wird in der Untersuchung der Begriff Verbraucher verwendet.

10 Vgl. §§ 33 ff. BDSG.

11 Vgl. § 34 Abs. 1 BDSG.

Daten deren Berichtigung verlangen. Zudem besteht in bestimmten Fällen ein Recht auf Löschung[12]. Es besteht weiterhin das Recht auf Sperrung, falls einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen[13]. Dies gilt auch, wenn durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden oder die Löschung nur mit unverhältnismäßig hohem Aufwand möglich ist.

Ziel ist es zu prüfen, ob Verbrauchern das Recht auf Auskunft gewährt wird, in welcher Weise die elektronischen Bezahldienstleister darauf reagieren und welche Inhalte die Auskunftsschreiben enthalten.

Verbrauchererwartung an den Datenschutz

Durch die Einwilligung sollen Verbraucher befähigt werden, eine freie Entscheidung über die Preis- und Weitergabe ihrer personenbezogenen Daten zu treffen. Dies ist nur möglich, wenn Verbraucher die Informationen in den Datenschutzerklärungen lesen und verstehen. Nur die Hälfte der Nutzer von Bezahldienstleistern gibt an, Datenschutzerklärungen zu lesen[14]. Ein Drittel der Leser bewertet die dort enthaltenen Informationen als nicht hilfreich[15]. Die Mehrheit der Nutzer dieser Verfahren ist somit nicht in der Lage, eine informierte Einwilligung zu geben.

Ziel ist es zu benennen, welche Informationen, Formate und Zeitaufwände Verbraucher präferieren, um hinreichend über den Umgang mit ihren Daten informiert zu sein.

Zur Operationalisierung der Zielstellungen werden im Folgenden konkrete Fragenstellungen formuliert. Diese werden mit Hilfe unterschiedlicher methodischer Herangehensweisen und Auswertungsmethoden untersucht und beantwortet. **Tabelle 1** (siehe Seite 12) stellt die Zielsetzung, die Fragestellungen und die Methodik im Überblick dar.

12 Vgl. hierzu § 35 Abs. 2 BDSG.
13 Vgl. § 35 Abs. 3 BDSG.
14 Vgl. Dautzenberg et al. (2017a), S. 31.
15 Vgl. ebenda.

METHODIK

Zur Untersuchung genannter Ziel- und Fragestellungen werden unterschiedliche methodische Ansätze und Vorgehensweisen gewählt. Diese werden nachfolgend skizziert und, wenn notwendig, im jeweiligen Ergebniskapitel detaillierter dargestellt.

Technische Analyse zur Datensicherheit und -sparsamkeit

Für die technische Analyse der Datensicherheit und -sparsamkeit wurde durch den Marktwächter Digitale Welt ein unabhängiges technisches Gutachten in Auftrag gegeben. Dieses wurde im Zeitraum zwischen dem 05.05. und 09.06.2017 durch die mgm security partners GmbH erstellt. In die Untersuchung einbezogen wurden die Bezahldienstleister Amazon Pay, giropay, paydirekt, PayPal, Skrill und SOFORT Überweisung. Es wurde keine Unterstützung durch die untersuchten elektronischen Bezahldienstleister angefragt. Diese wurden auch nicht im Vorfeld über die technische Prüfung benachrichtigt. Das Gutachten umfasste ausgewählte Sicherheitsaspekte, die im Rahmen einer Passivanalyse beobachtet werden können. Durch diese Limitierung konnten nicht alle relevanten Sicherheitsthemen[16] allumfassend berücksichtigt werden.

Die technische Plattform, die zur Durchführung der Tests verwendet wurde, bestand aus den Komponenten:

- Windows 7
- sslscan Version 1.11.10[17] unter Kali Linux
- Firefox Version 53.0.3
- Firefox ESR Version 45.9.0
- Burp Suite Professional Version 1.7.22

16 Auf Ebene der EU wird aktuell weiter über technische Anforderungen für die Sicherheit des Kontozugangs für Drittanbieter, die Zahlungsvorgänge auslösen können, diskutiert. Hierzu wurden von der Europäischen Bankenaufsicht regulative technische Standards formuliert (https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2). Risiken werden insbesondere darin gesehen, wenn bei der Nutzung Zugangsdaten weitergegeben werden, die, wenn sie unerkannt Unbefugten weitergeleitet werden, von diesen per Online-Banking ohne weiteres missbraucht werden können.
17 Das Programm sslscan Version 1.11.10 dient der Abfrage von SSL/TLS-Verschlüsselungsdiensten wie HTTPS und der Bestimmung der unterstützten Chiffren. Vgl. Linux Manpages Online (2017): sslscan, online verfügbar unter: https://man.cx/sslscan, Stand 07.08.2017.

1 ZIELSETZUNG, FRAGESTELLUNG UND METHODIK

Zielsetzung	Fragestellungen	Methodik
Datensicherheit (Kapitel 2)	• Wie sicher ist die Verschlüsselung der Kommunikation? • Wie sicher ist die Anmeldung beim Bezahldienstleister? • Wie erfolgt die technische Absicherung der Benutzersitzung? • Wie ist der effektive Schutz gegen Angriffe im Browser gestaltet? • Welche weiteren Schwachstellen wurden gefunden?	 Technische Analyse
Datensparsamkeit (Kapitel 3)	• Welche Daten werden während der Registrierung und des Bezahlprozesses erhoben? • Welche Tracking-Dienste verwenden die Bezahldienstleister?	
Transparenz (Kapitel 4)	• Welche rechtlichen Anforderungen gelten für Datenschutzerklärungen? • Wie wird in den Datenschutzerklärungen informiert? • Zu welchen Zwecken werden die Verbraucherdaten verwendet? • Wie verständlich sind Datenschutzerklärungen?	 Inhaltliche Analyse
Auskunftsrecht (Kapitel 5)	• Was beinhaltet das Recht auf Auskunft? • Wie reagieren Bezahldienstleister auf das Auskunftsverlangen? • Wie wird in den Auskunftsschreiben informiert? • Wie verständlich sind die Auskunftsschreiben?	 Verständlichkeits-analyse
Verbrauchererwartung (Kapitel 6)	• Welche Daten würden Verbraucher weitergeben? • In welchem Umfang wollen Verbraucher informiert werden? • In welcher Form wollen Verbraucher informiert werden? • Kennen und wünschen Verbraucher das Recht auf Auskunft?	 Verbraucherbefragung

Mit Hilfe der Software Burp Suite kann der Datenverkehr zwischen **Browser** des Nutzers und Web-Anwendung der Bezahldienstleister verfolgt werden. Die Browser schicken jeweils einen **HTTP-Header**, der den verwendeten Browser, die Version des Browsers sowie das verwendete Betriebssystem identifiziert. Über eine automatische Regel der Burp Suite wird der Header gegen Header des Internet Explorers Version 11 und Google Chrome Version 58.0.3029.81 ausgetauscht. Daher wurden in der Untersuchung die gängigen Browser Firefox, Internet Explorer und Google Chrome berücksichtigt. Die dargestellten Ergebnisse gelten für alle drei Konstellationen. Dies ergibt sich daraus, dass keine Veränderung gegenüber dem Referenzbrowser Firefox festgestellt wurde.

Im ersten Schritt wurden die **Programmierschnittstellen** der elektronischen Bezahldienstleister analysiert. Diese legen die Anbindung an das System fest und stellen es den Händlern in Form einer Dokumentation zur Verfügung. Nachfolgende Dokumentationen waren Untersuchungsgegenstand: Amazon Pay[18], giropay[19], paydirekt Checkout[20], PayPal Payments Standard[21], Skrill Quick Checkout[22] und SOFORT Überweisung[23].

18 Amazon Pay (2017): Amazon Pay API reference guide, online verfügbar unter: https://pay.amazon.com/de/developer/documentation/apireference/201751630, Stand 07.08.2017.

19 giropay (2017): GiroCheckout API, online verfügbar unter: http://api.girocheckout.de/girocheckout:giropay:start, Stand 07.08.2017.

20 paydirekt (2017): REST-API, paydirekt – Version 1.5, online verfügbar unter: https://www.paydirekt.de/haendler/merchant-api.html, Stand 07.08.2017.

21 PayPal (2017a): Payments API, online verfügbar unter: https://developer.paypal.com/docs/api/payments/, Stand 07.08.2017. PayPal bietet neben diesem Verfahren zwei weitere Verfahren zum Checkout an: PayPal Express Checkout (https://www.paypal.com/us/webapps/mpp/express-checkout, Stand 07.08.2017) und PayPal Payment Pro (https://www.paypal.com/us/webapps/mpp/paypal-payments-pro, Stand 07.08.2017). Diese beiden Verfahren waren nicht Bestandteil der Untersuchung.

22 Skrill (2017): Skrill Quick Checkout Integration Guide, online verfügbar unter: https://www.skrill.com/fileadmin/content/pdf/Skrill_Quick_Checkout_Guide.pdf, Stand 07.08.2017. Skrill bietet neben diesem Verfahren ein weiteres Verfahren zum Checkout an: Skrill Wallet (https://www.skrill.com/fileadmin/content/pdf/Skrill_Wallet_Checkout_Guide.pdf, Stand 07.08.2017). Dieses Verfahren war nicht Bestandteil der Untersuchung.

23 SOFORT GmbH (2016): SOFORT Überweisung – API Dokumentation, online verfügbar unter: https://www.sofort.com/integrationCenter-ger-DE/content/view/full/2513#hl, Stand 07.08.2017. SOFORT Überweisung bietet neben diesem Verfahren ein weiteres Verfahren zum Checkout an: SOROFT Überweisung Paycode (https://www.sofort.com/integrationCenter-ger-DE/content/view/full/3047, Stand 07.08.2017). Dieses Verfahren war nicht Bestandteil der Untersuchung.

Im zweiten Schritt fand eine Passiv-Analyse der Seiten der elektronischen Bezahldienstleister statt. Anschließend wurde für jeden Dienstleister, sofern möglich, mindestens ein Nutzerkonto erstellt. Im Folgenden wurden Testkäufe über diese Nutzerkonten abgewickelt und analysiert.

Verständlichkeitsanalyse zur Transparenz im Umgang mit Verbraucherdaten und Recht auf Auskunft

Verständlichkeit wird als das Zusammenwirken von Text- und Lesermerkmalen angesehen. Neben Eigenschaften des Lesers, wie individueller Lesefähigkeit und thematischer Vertrautheit, beeinflussen Textmerkmale, ob und wie die Bedeutung erfasst wird. Eigenschaften, wie die durchschnittliche Wort- und Satzlänge und syntaktische Komplexität der Sätze, wirken begünstigend oder erschwerend auf das Textverständnis[24]. Diese objektiven und quantifizierbaren Eigenschaften des Textes indizieren, wie schwierig es für den Leser tendenziell ist, einen Text zu verstehen.

Für die Analyse der Verständlichkeit wurde die Verständlichkeitssoftware TextLab verwendet. Die Software wurde von der H & H Communication Lab GmbH (comlab) in Kooperation mit der Universität Hohenheim entwickelt. Anhand verschiedener, validierter Lesbarkeitsformeln sowie bis zu 80 Kennzahlen werden formale Texteigenschaften, wie Wort- und Satzlänge und Worthäufigkeit, analysiert. Die Software identifiziert zudem Verstöße gegen die Verständlichkeit, wie beispielsweise lange oder verschachtelte Sätze, Passivkonstruktionen, Nominalstil oder Füllwörter. Für unterschiedliche Dokumentenarten (Brief, Fachtext oder Webtext) werden vom Programm spezifische Zielwerte vorgegeben.

Die Zielwerte der TextLab-Analyse beruhen dabei auf Studien des Instituts für Kommunikationswissenschaft der Universität Hohenheim[25] und orientieren

24 Vgl. Christmann/Groeben (1996): Textverstehen/Textverständlichkeit - ein Forschungsüberblick unter Anwendungsperspektive, in: Krings (Hg.): Wissenschaftliche Grundlagen der Technischen Kommunikation, Gunter Narr Verlag Tübingen, S.154f.

25 Eine Auflistung relevanter Studien findet sich unter: https://www.uni-hohenheim.de/organisation/einrichtung/fg-kommunikationswissenschaft-insbesondere-kommunikationstheorie?tx_base_lsfcontentadmin%5Baction%5D=listLsfPublicationsOfLsfInstitution&cHash=b5e4f94f6eb3352a970e7d842eff6f83.

sich an Gruppen mit formal niedrigerem Bildungsabschluss[26]. Aus den Text-Kennzahlen wird ein „Hohenheimer Verständlichkeitsindex“ (HIX) errechnet. Dieser ordnet die Verständlichkeit von Texten auf einer Skala von 0 „überhaupt nicht verständlich“ bis 20 „sehr leicht verständlich“ ein.

Zur Bewertung der Transparenz wird die Verständlichkeit der Datenschutzerklärungen und der Auskunftsschreiben mittels TextLab untersucht. Um die Vergleichbarkeit der Dokumente sicherzustellen, erfolgte eine Bereinigung der Dokumente nach Kriterien von comlab. Die Bereinigung wurde im Nachgang von comlab geprüft und bestätigt.

Inhaltliche Analyse der Transparenz im Umgang mit Verbraucherdaten und dem Recht auf Auskunft

Verbraucher können informierte Entscheidungen dann treffen, wenn sie vor Nutzung eines Dienstes hinreichend über Datenverwendung und Zweck informiert werden. Somit müssen die Bezahldienstleister über ein entsprechendes Informations- und Kommunikationsverhalten mit den Kunden Transparenz schaffen.

Zur Prüfung der Transparenz und Kommunikation zum Umgang mit persönlichen Verbraucherdaten wurden von einem Testkäufer jeweils drei Testkäufe mit den untersuchten Bezahldienstleistern durchgeführt. Die Testkäufe wurden zuvor bei verschiedenen Online-Händlern durchgeführt, je nach Bezahlverfahren mit oder ohne vorherige Registrierung. Kaufprozess und Registrierung wurden mittels Screenshots dokumentiert. Besonderes Augenmerk lag auf Hinweisen und Verlinkungen der geltenden Datenschutzerklärungen sowie der Forderung nach der rechtlich notwendigen Einwilligung in diese. Alle während des Prozesses verfügbaren Datenschutzerklärungen der Bezahldienstleister wurden gespeichert.

Nach dem Kauf wurden die Bezahldienstleister mittels eines standardisierten Musterbriefes[27] um Auskunft über den Umgang mit persönlichen Daten gebeten. Der Zeitraum der Untersuchung lag zwischen dem 27.07. und 04.10.2016. Das Musterschreiben wurde von jedem der sechs Testkäufer per E-Mail an den genutzten Dienstleister versendet. Das Schreiben wurde jeweils vom privaten E-Mail-Account der Testkäufer versandt. In dem Schreiben wurde um Rückmeldung innerhalb einer Zweiwochenfrist gebeten[28]. Erfolgte keine Reaktion des Bezahldienstleisters auf das Schreiben per E-Mail, wurde das Auskunftsverlangen mit erneuter Fristsetzung per Post übersandt. Forderte der Bezahldienstleister einen Identitätsnachweis der ersuchenden Person, wurde dieser zugesendet. Die Korrespondenz (E-Mails, Schreiben) wurde in elektronischer Form gespeichert und dokumentiert.

Die Datenschutzerklärungen wurden mittels inhaltlicher Analyse systematisch auf Angaben zur Datenverwendung bei Nutzung eines Bezahldienstleisters hin untersucht. Grundlage der inhaltlichen Bewertung waren die geltenden datenschutzrechtlichen Vorgaben[29]. Um eine bessere Vergleichbarkeit aller Bezahldienstleister zu gewährleisten, wurden die Regelungen des BDSG sowie des Telemediengesetz (TMG) zu Grunde gelegt. Ab 25. Mai 2018 finden die Regelungen der Datenschutzgrundverordnung (DSGVO)[30] sowie das BDSG-neu[31] Anwendung und ersetzen das bislang geltende BDSG. Eine Vorausschau auf die dann geltenden Rechtsvorschriften erfolgt an ausgewählten Stellen der Untersuchung. Soweit die Datenschutzerklärungen Regelungen über das Vertragsverhältnis zwischen Bezahldienstleister und Verbraucher beinhalten, werden Regelungen des Rechts der Allgemeinen Geschäftsbedingungen, §§ 305 ff. Bürgerliches Gesetzbuch (BGB), berücksichtigt.

26 Vgl. Brettschneider et al. (2014): Für Kunden oft schwer zu verstehen: Die Sprache der Banken 2014, online verfügbar unter: https://komm.uni-hohenheim.de/uploads/media/2014-08-03_Bankenstudie_01.pdf, Stand 07.08.2017, S.11.

27 Das Musteranschreiben ist abrufbar unter www.marktwaechter.de/digitale-welt/marktbeobachtung/e-payment-wie-sicher-sind-unsere-daten.

28 Für den Bezahldienstleister Skrill galt aufgrund seines Sitzes in Großbritannien eine Dreiwochenfrist.

29 Ob das Bundesdatenschutzgesetz (BDSG) Anwendung findet, richtet sich danach, wo personenbezogene Daten erhoben werden. So gilt für Unternehmen mit Niederlassung in der Europäischen Union nicht das BDSG, soweit die personenbezogenen Daten in der EU erhoben und verarbeitet werden (vgl. § 1 Abs. 5 S. 1 BDSG). Für diese Unternehmen gelten die nationalen Regelungen des jeweiligen Mitgliedsstaates. Anhand der vorliegenden Datenschutzerklärungen fand eine Zuordnung zur jeweils geltenden Rechtsordnung statt. Für Amazon Pay und PayPal gilt luxemburgisches Recht und für Skrill die Datenschutzvorschriften für Großbritannien.

30 Die Verordnung findet unmittelbar in allen EU-Mitgliedstaaten Anwendung und dient der Vereinheitlichung des europäischen Datenschutzrechts.

31 Vgl. Art. 1 des Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680.

Verbraucherbefragung zur Erwartung an den Datenschutz

Im Auftrag des Marktwächters Digitale Welt wurde durch die forsa.main Marktinformationssysteme GmbH eine Befragung zu Erwartungen von Nutzern elektronischer Bezahlverfahren durchgeführt. Die Untersuchung fand im Erhebungszeitraum vom 07. bis 16.07.2017 statt. Ziel der Befragung war, konkrete Verbrauchermeinungen zu folgender Thematik zu erhalten: In welcher Form und über welche Inhalte möchten Verbraucher bei der Nutzung ihrer persönlichen Daten durch die Bezahldienstleister informiert werden? Um die Erwartungen möglichst unvoreingenommen zu erheben, wurden zunächst offene Fragen gestellt. Diese wurden dann in einem zweiten Schritt durch geschlossene Fragen ergänzt.

Die Fragenkomplexe richteten sich auf folgende Aspekte: Welche persönlichen Daten wollen Verbraucher weitergeben? Welche Informationsformate präferieren Verbraucher? Wie viel Zeit würden sie zum Lesen von Datenschutzerklärungen aufbringen? Ein weiterer Fragenkomplex erfasste, ob die Nutzer von ihrem Recht auf Auskunft wissen und davon Gebrauch machen wollen.

Zielgruppe der Befragung waren Nutzer elektronischer Bezahlverfahren ab 18 Jahren in den Privathaushalten in Deutschland. Dazu wurde eine repräsentative Zufallsauswahl deutschsprachiger Internetnutzer zu Beginn der Befragung auf die Nutzung elektronischer Bezahlverfahren gescreent und selektiert[32]. Demografische Daten wurden zu Geschlecht, Alter, Region, Bildung, Haushaltsgröße und Haushaltsnettoeinkommen erhoben. Die finale Gesamtstichprobe umfasste 2.001 Personen mit einer statistischen Fehlertoleranz von +/- 2 Prozentpunkten. Die Befragung erfolgte anhand eines strukturierten Fragebogens[33] mittels computergestützter Webinterviews (CAWI) im Online-Panel forsa.omninet.

32 Frage: Wenn Sie an das Einkaufen und Bezahlen im Internet denken: Nutzen Sie zumindest gelegentlich einen Bezahldienstleister, wie zum Beispiel PayPal, SOFORT Überweisung, Amazon Pay, paydirekt oder giropay, bei der Bezahlung von Waren und Dienstleistungen, die Sie im Internet kaufen?

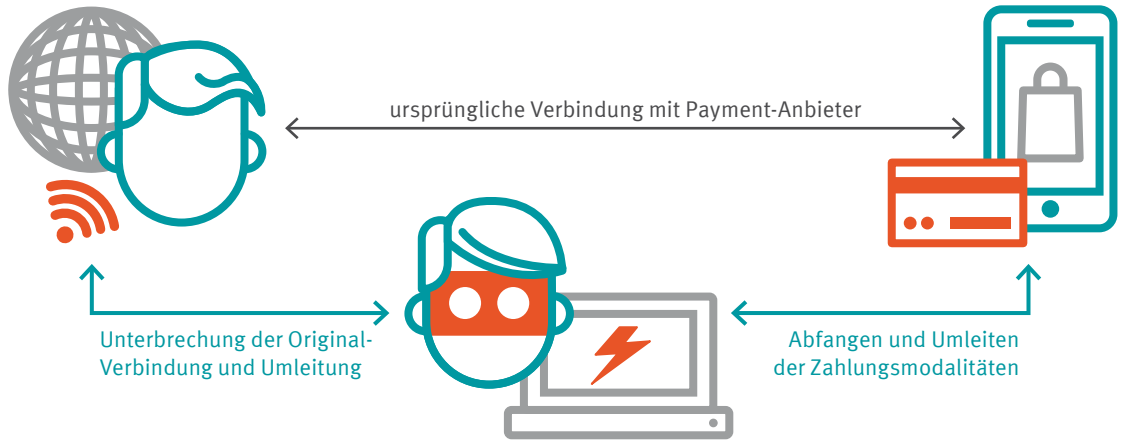
33 Der Fragebogen ist abrufbar unter www.marktwaechter.de/digitale-welt/marktbeobachtung/e-payment-wie-sicher-sind-unsere-daten.

2. DATENSICHERHEIT

Die Datensicherheit und damit die Angst vor Missbrauch durch kriminelle Dritte ist für Verbraucher der kritischste Punkt bei der Nutzung elektronischer Bezahlverfahren[34]. Erklärtes Ziel von Datensicherheit ist der Schutz vor dem Zugriff auf personenbezogene Daten von außen[35]. Die Gewährleistung der Sicherheit in der Informationstechnik verfolgt die Einhaltung bestimmter Sicherheitsstandards[36]. Diese dienen der Wahrung der Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen mittels Sicherheitsvorkehrungen[37]. Die elektronischen Bezahldienstleister müssen somit sicherstellen, dass bei der Nutzung des Dienstes von außen auf keine personenbezogenen Daten zugegriffen wird. Mittels technischer Analyse wurde die Datensicherheit geprüft.

Um zu ermitteln, inwiefern elektronische Bezahldienstleister gängigen Datensicherheitsstandards genügen, wurden im **Frontend** für drei Browser[38] relevante Sicherheitsaspekte geprüft. Hierbei wurden ausschließlich defensive und passive Maßnahmen ergriffen[39]. Besonderes Augenmerk lag auf den unterschiedlichen Sicherheitsmerkmalen zum Schutz der Web-Kommunikation zwischen den Kunden und den Bezahldienstleistern. Es ging vor allem darum, potenzielle Angriffsmöglichkeiten durch einen sogenannten **Man-in-the-Middle** auszuschließen. **Abbildung 2** stellt die Angriffsmöglichkeit grafisch dar. Die untersuchten Aspekte bezogen sich auf: (1) die Verschlüsselung der Kommunikation zwischen dem Browser des Nutzers und dem Bezahldienstleister, (2) die Anmeldung beim Bezahldienstleister, (3) die Absicherung der **Benutzersitzung** während des Zahlvorganges und (4) den Schutz gegen Angriffe im Browser des Nutzers.

2 MAN-IN-THE-MIDDLE-ANGRIFF



Man in the Middle
gibt sich beim Käufer als Verkäufer und beim Verkäufer als Käufer aus

34 Vgl. Dautzenberg et al. (2017a), S. 5 ff.
35 Vgl. Schröder (2016): Datenschutzrecht für die Praxis, 2. Auflage, dtv.
36 Vgl. § 2 Absatz 2 BSIG.
37 Vgl. ebenda.
38 Mozilla Firefox, Google Chrome, Internet Explorer.
39 Ein Penetrationstest wurde nicht durchgeführt.

WIE SICHER IST DIE VERSCHLÜSSELUNG DER KOMMUNIKATION?

Zur sicheren Verschlüsselung der Kommunikation zwischen Browser des Nutzers und **Server** des Bezahldienstleisters gehört, dass keine als verwundbar bekannte Konfiguration eingesetzt wird. Andernfalls bestünde für einen potentiellen Angreifer die Möglichkeit, Einfluss auf den Verbindungsprozess zu nehmen und eine unsichere Konfiguration herbeizuführen. Ein Server bietet in der Regel mehrere mögliche Konfigurationen an. Im Rahmen des Verbindungsaufbaus einigt sich dann der Browser des Kunden mit dem Server auf eine genutzte Konfiguration. Die angebotenen Konfigurationen lassen sich in den Protokollen **Transport Layer Security (TLS)** hinsichtlich der Sicherheitsaspekte Authentizität (des Kommunikationspartners), Integrität (der transportierten Daten) und Vertraulichkeit prüfen.

Die Prüfung wurde für die sechs elektronischen Bezahlverfahren mittels sslcan Version 1.11.10 durchgeführt. Geprüft wurden die Verschlüsselungsstandards zur Etablierung des Kanals über **HTTPS**, zum Austausch der Daten über den etablierten Kanal und zur Sicherung der Datenintegrität auf dem Kanal. Weiterhin wurden die Länge des verwendeten Schlüssels, die Sicherstellung des verschlüsselten Kanals über **HSTS** sowie der Authentizitätsnachweis über ein **Extended-Validation-SSL-Zertifikat** geprüft. Die Ergebnisse sind vor dem Hintergrund zu interpretieren, dass in den letzten Jahren Angriffe auf bis dato häufig eingesetzte Verschlüsselungsverfahren bekannt geworden sind. Diese betrafen in der Regel einzelne Konfigurationen, von deren Verwendung spätestens ab Bekanntwerden abzuraten ist.

Im Ergebnis erlaubte jeweils jeder Server der untersuchten Bezahldienstleister, einen als gebrochen angesehenen Verschlüsselungsstandard (TLSv1.0) einzusetzen. Moderne Browser sind für bekannte Angriffe auf dieses Protokoll nicht mehr anfällig. Dennoch empfiehlt das Bundesamt für Sicherheit in der Informationstechnik (BSI), diese Version abzuschalten[40]. Häufig wird diese Version jedoch angeboten, da sonst ältere Systeme[41] nicht mehr mit dem Server kommunizieren können. Amazon Pay, paydirekt, PayPal und SOFORT Überweisung stellen bei der Kommunikation zwischen Browser und Server sicher, dass alle Daten immer mit HTTPS verschlüsselt übertragen werden. Erkennbar ist dies durch den Beginn der Adresszeile mit „https“ im Browser. Giropay und Skrill wiesen hier deutliche Lücken auf. So wurde bei beiden zum Zeitpunkt der Untersuchung die verschlüsselte Kommunikationsaufnahme zum Server nicht forciert (kein HSTS). Immerhin wurde, nachdem ein Nutzer eine unverschlüsselte Anfrage mit HTTP schickte, dieser zum verschlüsselten HTTPS weitergeleitet. Dennoch bestand die Möglichkeit, dass ein Angreifer die Weiterleitung unterbinden und dafür sorgen konnte, dass kein verschlüsselter Kanal aufgebaut wird (**SSL-Stripping-Angriff**). Erkennbar ist dies am fehlenden Sicherheitsschloss im Browser[42]. **Abbildung 3** (Seite 18) stellt den Ablauf eines SSL-Stripping-Angriffs dar. Beide Bezahldienstleister wurden darüber informiert: Giropay löste dieses Problem umgehend zum 01.08.2017[43].

Von Skrill liegt bis zum Redaktionsschluss keine Rückantwort zur Lösung des Problems vor. Daher kann derzeit nicht von einer Lösung ausgegangen werden.

Die Sicherheit des Kommunikationskanals wird über eine **Chiffrierung** bzw. Verschlüsselung gewährleistet. Hierzu bedient man sich verschiedener mathematischer Algorithmen. Diese gelten als sicher, wenn sie bis heute allen **Kryptoanalysen** erfolgreich widerstanden haben. Amazon Pay, paydirekt, Skrill und SOFORT Überweisung nutzen durchweg sichere Chiffren. Sowohl giropay als auch PayPal verwendeten zum Zeitpunkt der Prüfung einen unsicheren Algorithmus. Auch hierüber wurden die Bezahldienstleister informiert: Giropay löste dieses Problem umgehend zum 01.08.2017[44].

PayPal reagierte auf dreimalige Anfrage per E-Mail nicht[45]. Von einer Lösung des Problems kann nicht ausgegangen werden.

40 Vgl. Bundesamt für Sicherheit und Informationstechnik (BSI) (2017a): BSI-TR-02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, online verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf, Stand 07.08.2017, S. 5.

41 Wie beispielsweise Internet Explorer und Windows XP.

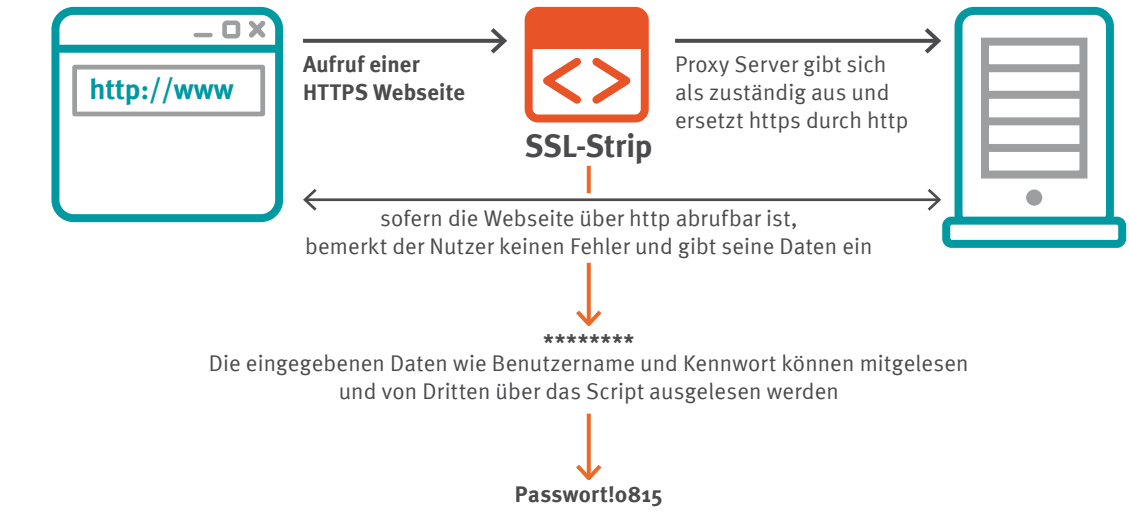
42 Allerdings lässt sich dieses auch nachahmen. Die Erkennung erfordert die Aufmerksamkeit des Nutzers für diese Gefahr. Da der Browser keine Warnung ausgibt, wird ein solcher Angriff vom Nutzer leicht übersehen.

43 Mail von giropay vom 02.08.2017.

44 Mail von giropay vom 02.08.2017.

45 Es erfolgten Anfragen per E-Mail am 18.07.2017, 21.07.2017 und 27.07.2017 jeweils an die Adresse kundenbetreuung@paypal.com.

3 SCHEMATISCHE DARSTELLUNG EINES SSL-STRIPPING-ANGRIFFS



Alle untersuchten Bezahldienstleister setzen ein Extended-Validation-SSL-Zertifikat ein. Dieses symbolisiert eine besonders vertrauensvolle Kommunikation. Erkennbar ist das Zertifikat an der grün hinterlegten Adresszeile des Browsers.

WIE SICHER IST DIE ANMELDUNG BEIM BEZAHLDIENSTLEISTER?

Nachfolgend wird der Frage nachgegangen, inwiefern eine sichere Anmeldung (Login) bei den untersuchten Bezahldienstleister möglich oder sogar verpflichtend ist. Dabei wird eine Standard-Anmeldung mit Benutzername und Passwort als Maßstab zugrunde gelegt und geprüft, ob eine **2-Faktor-Authentifizierung** angeboten wird. Auch wird untersucht, ob die Bezahldienstleister einen Schutz gegen **Phishing-Angriffe** während des Einkaufs bieten. Hierbei würde sichergestellt, dass der Kunde mit der echten Webseite des Dienstleisters und nicht mit einer gefälschten Seite kommuniziert.

Amazon Pay, PayPal und Skrill bieten dem Kunden bei Anmeldung einen zusätzlichen optionalen Schutz über eine 2-Faktor-Authentifizierung mit SMS-TAN. Sofern der Nutzer den zusätzlichen Schutz aktiviert, bekommt er für jede Anmeldung eine SMS mit einer TAN. Erst nach Eingabe der TAN ist er in seinem Konto angemeldet. Amazon Pay und PayPal schützen die aktuelle Nutzersitzung zusätzlich, indem die Sitzung an den aktuell verwendeten Browser geknüpft wird. Meldet man sich in zwei verschiedenen Browsern beim Bezahldienstleistern an, so ist nur die letzte Anmeldung gültig. Die erste Anmeldung im anderen Browser wird invalidiert, der Nutzer wird zur Login-Seite weitergeleitet. Das Benutzerkonto bei paydirekt ist immer direkt mit einem Online-Banking-Konto verknüpft. Für die Anmeldung werden Benutzername und Passwort verlangt. Der Abschluss einer Transaktion wird durch eine TAN des verknüpften Bankkontos geschützt. Giropay und SOFORT Überweisung verlangen keine Registrierung und erfordern somit keine Anmeldung.

Alle implementierten Einkaufsverfahren der Bezahldienstleister sind prinzipiell anfällig für Phishing-Angriffe. Das Problem besteht, da der Händler den Kunden zur Anmeldeseite des Bezahldienstleisters weiterleitet. Jeder Dritte könnte die Seite des vom Kunden gewählten Dienstleisters prinzipiell fälschen und auf diese weiterleiten. Der Kunde merkt von diesem Vorgang nichts, solange er nicht sorgfältig die Adresszeile des Browsers im Blick behält und die korrekte Adresszeile auch kennt. Gegenmaßnahmen sind am Markt bisher nicht etabliert oder befinden sich – nach dem Kenntnisstand des technischen Gutachters – im Proof-of-Concept-Stadium.

WIE ERFOLGT DIE TECHNISCHE ABSICHERUNG DER BENUTZERSITZUNG?

Nachfolgend wird geprüft, wie die **Benutzersitzung** (Session) durch die Bezahldienstleister geschützt wird. Das Login erfolgt in der Regel über die Eingabe eines Nutzernamens[46] und eines Passworts. In der Zeit zwischen Login und Logout sind dem Nutzer zurechenbare Aktionen ohne Eingabe des Passworts möglich. Im ersten Schritt wird untersucht, wie ein Geheimnis, das für die Phase der Session das Passwort ersetzt, bei den Bezahldienstleistern implementiert wird. Das üblichste Verfahren nutzt hierfür **Cookies**. Diese speichern das Geheimnis (die Session ID) und werden automatisch mit jeder Anfrage an den Dienstleister übertragen. Die Cookies müssen gegen den unberechtigten Zugriff Dritter durch **Cross-Site Scripting (XXS)** oder Man-in-the-Middle-Angriffe geschützt werden. Die entsprechenden Schutzmaßnahmen werden nachfolgend untersucht.

Die erforderliche Konfiguration der Sitzungscookies von Amazon Pay, PayPal und Skrill weist keine erkennbaren Mängel auf. Die Cookies sind durch das Setzen entsprechender Schutz-Attribute (HttpOnly, secure), die das Stehlen oder Manipulieren verhindern sollen, geschützt. Zudem ist das Cookie nur solange gültig, wie der Browser geöffnet ist. Daneben wird die aktive Session nach einer hinreichend kurzen Zeit (maximal 2 Stunden) der Inaktivität[47] serverseitig invalidiert. Die Cookie-Konfiguration von Amazon Pay weist eine Abweichung auf: Sitzungsrelevante Cookies sind seitens des **Clients** bis in das Jahr 2037 gültig. In dem Fall löscht der Browser die Cookies beim Schließen nicht. Er behält diese nach Neustart bis zur Erreichung des Datums oder dem Überschreiben durch Amazon Pay bei. Auch hier konnte jedoch festgestellt werden, dass die Nutzersitzung nach einer hinreichend kurzen Zeit (maximal 2 Stunden) serverseitig invalidiert wurde. Paydirekt setzt bei der Absicherung der Benutzersitzung auf eine moderne Architektur: Hier werden **Tokens** (Zeichenketten) als Authentifizierungsmerkmal im Speicher des Browsers abgelegt. Diese werden beim Schließen des Browsers automatisch gelöscht. Im Fall eines Cross-Site Scripting Angriffs sind sie jedoch ungeschützt und könnten aus dem Browser des Nutzers entführt werden[48]. Paydirekt wurde darüber informiert. Das Unternehmen führte aus, dass „neben der … **Content Security Policy (CSP)**, die Validierung der Eingaben, das Unterbinden von ausführbarem Code sowie eine begrenzte Gültigkeit und Session bezogene Verwendbarkeit des erzeugten Tokens“ als „wirksame Maßnahmen gegen Cross Site Scripting (XSS)-Attacken in eigenen Penetrationstests geprüft wurden“[49]. Bei den Dienstleistern giropay und SOFORT Überweisung wird keine Benutzersitzung basierend auf einer Authentifizierung aufgebaut.

WIE IST DER EFFEKTIVE SCHUTZ GEGEN ANGRIFFE IM BROWSER GESTALTET?

Die Implementierung einer Content Security Policy (CSP) ist ein zusätzlicher technischer Schutz gegen Angriffe, die im Browser des Kunden stattfinden können. Dadurch können mögliche, von Angreifern eingeschleuste Funktionen erkannt und unterbunden werden. Die Policy wird vom Bezahldienstleister definiert und per HTTP-Header an den jeweiligen Browser des Kunden ausgeliefert. Dort wird die Einhaltung überwacht und sichergestellt. Es wurde geprüft, ob und welche Policy durch die Dienstleister eingesetzt wird.

Die wesentlichen Funktionen von Amazon Pay werden über die Domain pay.amazon.com abgewickelt und liefern eine CSP. Auffällig ist, dass alle Quellen und damit verfügbare Inhalte anderer Seiten erlaubt werden. Damit ist die Ausführung von Skripten nicht eingeschränkt. Es werden auch keine Einschränkungen für **Browser-Erweiterungen** wie Plug-Ins gemacht. Der CSP-Evaluator von Google[50] meldet hier zwei definitive und ein mögliches Sicherheitsrisiko. Die Policy von paydirekt beschränkt erlaubte Quellen auf wenige und scheinbar eigene Dienste wie „d.paydirekt.de“ und „api.paydirekt.de“. Der CSP-Evaluator von Google erkennt keine Sicherheitsrisiken. PayPal verwendet ebenfalls eine CSP. Diese öffnet sich neben **Hosts** aus dem eigenen Universum auch Drittanbietern wie Youtube. Der CSP-Evaluator von Google moniert im Wesentlichen die Offenheit für die Ausführung von **JavaScript**,

46 Häufig wird die E-Mail-Adresse als Nutzername verwendet.
47 Die Länge der Zeitdauer wurde nicht konkret gemessen.
48 Vgl. National Institute of Standards and Technology (NIST) (2017): Digital Identity Guidelines, online verfügbar unter: https://pages.nist.gov/800-63-3/sp800-63b.html#sec7, Stand 07.08.2017.
49 Mail von paydirekt vom 25.07.2017.
50 Vgl. Google (2017): CSP Evaluator, online verfügbar unter: https://csp-evaluator.withgoogle.com/, Stand 07.08.2017.

welches Grundlage für oben geschilderte Angriffe ist. Giropay, Skrill und SOFORT Überweisung verwenden keine Content Security Policy als zusätzlichen Schutz gegen Angriffe.

WELCHE WEITEREN SCHWACHSTELLEN WURDEN GEFUNDEN?

Giropay gibt durch seine HTTP-Header seine verwendeten Technologien inklusive Versionsnummern der eingesetzten Software preis[51]. Dieser Zustand ist insofern bedenklich, als dass daraus auf bestehende Verwundbarkeiten in der Software geschlossen werden kann. Entsprechende Verwundbarkeiten können leicht über Suchmaschinen gefunden werden. Giropay hat das Problem auf Hinweis des Marktwächters Digitale Welt zum 01.08.2017 behoben[52]. SOFORT Überweisung verwendete zum Zeitpunkt der Untersuchung eine als verwundbar bekannte JavaScript-**Bibliothek**[53]. Die Schwachstellen sind u.a. hier dokumentiert[54]. Sie erlauben sogenannte XSS-Angriffe auf die Nutzer der Seite. SOFORT Überweisung wurde darüber informiert und hat die Schwachstelle umgehend beseitigt. Es wurde zudem angekündigt, eine außerordentliche Sicherheitsprüfung der Webseite bei einem externen IT-Security Dienstleister zu veranlassen[55].

FAZIT: HOHES SICHERHEITSNIVEAU WIRD GEWÄHRLEISTET

Das Ergebnis zeigt: Die untersuchten elektronischen Bezahldienstleister entsprechen im Großen und Ganzen ihrer Verantwortung nach Datensicherheit für die Nutzer. Es wird ein vergleichsweise hohes Sicherheitsniveau festgestellt. Die Verschlüsselung der Kommunikation zwischen dem Browser des Nutzers und dem Server des elektronischen Bezahldienstleisters wird als sicher eingeschätzt. Alle Bezahldienstleister setzen zudem ein Extended-Validation-SSL-Zertifikat ein. Alle elektronischen Bezahldienstleister bieten zur sicheren Anmeldung eine 2-Faktor-Authentifizierung, wie zum Beispiel über SMS-TAN, an. Bei paydirekt erfolgt die 2-Faktor-Authentifizierung bei Abschluss der Zahlung. Ein wirksamer Schutz gegen beschriebene Phishing-Angriffe ist nicht implementiert. Dieser ist erst zu erwarten, wenn es bereits eine nennenswerte Anzahl von Missbrauchsfällen gegeben hat. Dies entspricht dem Prinzip der reaktiven Sicherheit. Die Benutzersitzung ist bei jedem untersuchten Bezahldienstleister sehr gut geschützt. Der technische Gutachter konstatiert: Im Vergleich zu allgemeinen Web-Anwendungen besteht ein deutlich höheres Sicherheitsniveau bei den elektronischen Bezahlverfahren.

Hinsichtlich der CSP zeigt sich ein gemischtes Bild: Die Policy von paydirekt ist als gut zu bewerten. PayPal und Amazon Pay machen mit ihrer CSP sichtbare Kompromisse. Giropay, SOFORT Überweisung und Skrill haben keine CSP implementiert. Einschränkend muss gesagt werden, dass die Einführung einer CSP für ältere Web-Anwendungen meist mit erheblichem Aufwand verbunden ist. Neuere Varianten der CSP senken die Einstiegshürden zwar, werden aber noch nicht von allen Browsern unterstützt.

51 Server: Apache/2.4.7 (Ubuntu) X-Powered-By: PHP/5.5.9-lubuntu4.21 [...] X-Generator: Drupal 7 (http://drupal.org).
52 Mail von giropay vom 02.08.2017.
53 prettyPhoto v3.1.4, eingebunden auf: https://www.sofort.com/integrationCenter-eng-DE/integration/.
54 NIST (2013): CVE-2013-6837 Detail, online verfügbar unter: https://nvd.nist.gov/vuln/detail/CVE-2013-6837, Stand 07.08.2017.
55 Mail von SOFORT Überweisung vom 27.07.2017.

3. DATENSPARSAMKEIT

Neben der Datensicherheit war es insbesondere der Unwille „persönliche Daten offenzulegen“, der Online-Käufer davon abhält, elektronische Bezahlverfahren zu nutzen[56]. Auch seitens der Nutzer dieser Verfahren bestehen hinsichtlich der Verarbeitung ihrer personenbezogenen Daten Bedenken[57]. Dennoch ist es bei der Nutzung elektronischer Bezahldienstleister unumgänglich, Daten zu erheben und zu verarbeiten. Bei der Registrierung und bei der Bezahlung fallen personenbezogene, personenbeziehbare und nicht personenbezogene Daten an. Personenbezogene Daten sind Informationen, die sich auf eine bestimmte Person beziehen und diese identifizierbar machen, beispielsweise Name oder E-Mail-Adresse[58]. Personenbeziehbare Daten ermöglichen mittelbar ebenfalls die Identifikation einer Person[59]. Ein Beispiel für ein personenbeziehbares Datum ist die Ausweisnummer. Nicht personenbezogene Daten lassen dahingegen keinen Rückschluss auf eine Person zu[60].

Bei der Nutzung digitaler Dienste, wie elektronische Bezahlverfahren, fällt es den Menschen immer schwerer nachzuvollziehen, was mit ihren betreffenden Daten geschieht[61]. Die strikte Einhaltung des Prinzips der Datensparsamkeit[62] kann hier für Vertrauen bei den Verbrauchern werben. Konkret bedeutet dies, dass die während der Registrierung und Bezahlung vom Nutzer geforderten Daten durch den Bezahldienstleister auf das notwendigste Maß zur Absicherung des Dienstes beschränkt werden. Auch durch Anonymisierung oder Pseudonymisierung erhobener Daten kann die Privatheit des Einzelnen gewährleistet werden. Eine Einbindung von Tracking-Diensten durch die Bezahldienstleister sollte auf ein notwendiges Maß zur Optimierung der Kundenfreundlichkeit des Dienstes beschränkt werden und die Verwendung der Daten sollte mindestens in pseudonymisierter Form erfolgen.

Daher wird im nächsten Schritt dargelegt, inwiefern die Bezahldienstleister dem Prinzip der Datensparsamkeit im Rahmen der Gestaltung ihrer Registrierungs- und Bezahlprozesse sowie durch den sparsamen Einsatz von Tracking-Diensten nachkommen.

WELCHE DATEN WERDEN WÄHREND DER REGISTRIERUNG UND DES BEZAHLPROZESSES?

Für die Nutzung der Bezahldienstleister Amazon Pay, PayPal, paydirekt und Skrill müssen sich Nutzer im Vorfeld registrieren und dabei Daten an den Dienst übermitteln. Giropay und SOFORT Überweisung führen keine Nutzerkonten, eine Registrierung ist daher nicht erforderlich. Neben der Registrierung erhalten die Bezahldienstleister während des Bezahlprozesses Daten des Nutzers. Zum einen erfassen die Bezahldienstleister selbst Daten der Nutzer. Zum anderen übermitteln die Händler Nutzerdaten, die diese beim Kauf erheben. Welche Daten vom Händler an den Bezahldienstleister übermittelt werden, legt der jeweilige Bezahldienstleister fest und stellt den Händlern diese Festlegung mittels seiner Dokumentation zur Verfügung (vgl. Kapitel 1). Nachfolgende Auswertung der einzelnen Bezahldienstleister berücksichtigt alle Arten erhobener Daten bei Registrierung und Bezahlung.

Amazon Pay

Bei der Registrierung gibt der Nutzer Vor- und Nachname, E-Mail-Adresse und Passwort an. Weitere Daten, wie Anschrift, Telefonnummer und Zahlungsmittel, fragt Amazon Pay im Zuge des ersten Einkaufs beim Kunden direkt ab. Bei jedem nachfolgenden Einkauf und Bezahlprozess loggt sich der Nutzer mit E-Mail-Adresse und Passwort ein und bestätigt, dass Amazon Pay Namen, E-Mail-Adresse, Versand- und Rechnungsadressen an den Händler übermitteln darf. Der Händler gibt bei der Zahlung den Zahlungsbetrag und optional die E-Mail-Adresse an den Bezahldienstleister weiter.

56 Vgl. Dautzenberg et al. (2017a), S. 5 ff.
57 Vgl. ebenda.
58 Vgl. Gola/Klug/Körffer (2015): Bundesdatenschutzgesetz, 12. Auflage, C.H.Beck, BDSG § 3, Rn. 3.
59 Vgl. Schild (2017), in Wolff/Brink (Hg.): BeckOK Datenschutzrecht, 20. Auflage, C.H.Beck, BDSG § 3, Rn. 19.
60 Vgl. Gola/Klug/Körffer (2015), BDSG § 3, Rn. 3.
61 Vgl. Schaar (2017): Verbraucherdatenschutz in der Digitalisierung, Herausforderungen und Lösungsansätze, Friedrich-Ebert-Stiftung, online verfügbar unter: http://library.fes.de/pdf-files/wiso/13497.pdf, Stand 07.08.2017, S. 1.
62 Vgl. BDSG § 3a: „Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen.“

Amazon Pay können Verbraucher nur nutzen, wenn sie über ein Amazon-Nutzerkonto verfügen. Andernfalls wird dieses bei Registrierung erstellt. Daten aus einem bestehenden Nutzerkonto bei Amazon sind somit für den Bezahldienstleister verfügbar.

giropay

Für die Nutzung von giropay ist keine Registrierung durch den Nutzer notwendig. Daher wird bei einer Zahlung zunächst geprüft, ob die Bank des Nutzers Bankpartner von giropay ist[63]. Hierfür leitet der Händler den Bank Identifier Code (BIC) des Nutzers an giropay weiter. Nach erfolgreicher Prüfung des BIC übermittelt der Händler Zahlungsbetrag und Währung an den Bezahldienstleister. Zudem kann der Händler optional die International Bank Account Number (IBAN) sowie weitere, von ihm ausgewählte Informationen übertragen. Hierfür stehen dem Händler fünf Felder mit frei definierbarem Text zur Verfügung. Die in diesen Feldern eingegebenen Informationen werden den Nutzern bei der Überweisung angezeigt. Der Nutzer muss giropay bei der Bezahlung das Land der Bank, BIC, Zugangsnummer und PIN für das Online-Banking seiner Bank sowie eine Transaktionsnummer (TAN) mitteilen.

paydirekt

Paydirekt erhebt bei der Registrierung vom Nutzer Vor- und Nachname, Anschrift, Geburtsdatum, Telefonnummer, E-Mail-Adresse, Kontodaten (IBAN und BIC), die verwendete Währung, Benutzername und Passwort. Während des Zahlungsvorgangs muss sich der Nutzer mit Benutzername und Passwort identifizieren. Vom Händler erhält paydirekt bei der Zahlung die Versandadresse und den Zahlungsbetrag mit Währung. Optional kann der Händler Angaben zur gekauften Ware (Anzahl, Name, Preis, europäische Artikelnummer (EAN)), E-Mail-Adresse, Kundennummer und Versandinformationen (Paketdienstleister, Sendungsnummer, voraussichtliches Versanddatum) an den Bezahldienstleister übermitteln.

63 Die Bankpartner von giropay sind: Sparkassen, Volks- und Raiffeisenbanken, Postbank, comdirect, BB Bank, MLP, psd Bank und DKB.

PayPal

Bei der Registrierung verlangt PayPal vom Nutzer die Eingabe von Vor- und Nachname, Anschrift, Land, Geburtsdatum, Telefonnummer, E-Mail-Adresse, Nationalität sowie Passwort. Beim Bezahlen loggt sich der Nutzer mit E-Mail-Adresse und Passwort ein. Vom Händler bekommt PayPal bei der Zahlung E-Mail-Adresse, Informationen zur gekauften Ware (Anzahl, Name, Beschreibung, Preis, Mehrwertsteuer, Artikelnummer (SKU)), den Zahlungsbetrag mit Währung sowie Versand-/Rechnungsadresse des Nutzers. Der Händler kann zudem optional Anrede, Vor- und Nachname, Anschrift, Geburtsdatum, Telefonnummer, Kreditkartendaten sowie Steuernummer im Zuge der Bezahlung an PayPal geben.

Skrill

Der Nutzer gibt bei der Registrierung Vor- und Nachname, Anschrift, Land, Geburtsdatum, Telefonnummer, Passwort und verwendete Währung an. Optional kann der Nutzer bei der Registrierung zudem eine zweite Anschrift eintragen. Bei der Zahlung identifiziert sich der Nutzer mit E-Mail-Adresse und Passwort. Der Händler muss bei der Bezahlung zwingend nur den Zahlungsbetrag an Skrill übermitteln. Daneben hat der Händler die Option, Vor- und Nachname, Anschrift, Geburtsdatum, Telefonnummer und E-Mail-Adresse des Nutzers an den Bezahldienstleister weiterzugeben.

SOFORT Überweisung

Für die Nutzung von SOFORT Überweisung ist keine Registrierung durch den Nutzer notwendig. Der Nutzer gibt beim Bezahlen das Land seiner Bank, BIC (oder Bankleitzahl (BLZ)), Zugangsnummer und PIN für das Online-Banking sowie eine TAN an[64]. Optional kann der Nutzer seine E-Mailadresse eingeben, um eine Trans-

64 Gemäß dem Urteil vom 18.07.2017, KZR 39/16 des Bundesgerichtshofes ist SOFORT Überweisung als einzig kostenlose Zahlungsweise nicht zumutbar. Hintergrund der Entscheidung ist, dass als einzige kostenlose Zahlungsart Verbraucher nicht dazu gezwungen werden dürfen, mit einem nicht beteiligten Dritten in vertragliche Beziehungen zu treten und hochsensible Finanzdaten zu übermitteln, zumal dies gegen die vertragliche Vereinbarung mit ihrer Bank verstoße. Als Geschäftsmodell ist der Bezahldienstleister zulässig. Vgl. Verbraucherzentrale Bundesverband (vzbv): BGH stärkt Kundenrechte beim Bezahlen im Internet, online verfügbar unter: http://www.vzbv.de/pressemitteilung/bgh-staerkt-kundenrechte-beim-bezahlen-im-internet, Stand 08.08.2017.

aktionsbestätigung per E-Mail zu erhalten. Der Händler muss bei der Bezahlung nur Zahlungsbetrag mit Währung an den Bezahldienstleister übermitteln. Optional kann der Händler Kontodaten (Kontoinhaber, IBAN, BIC (oder alternativ Kontonummer und BLZ)), E-Mail-Adresse und Telefonnummer des Nutzers an SOFORT Überweisung weiterleiten.

Tabelle 4 fasst alle im Zuge der Registrierung und Bezahlung erfassten Daten durch den Bezahldienstleister und Händler zusammen. Die Anzahl der Daten, die vom Nutzer übermittelt werden müssen, variiert zwischen vier und 13 Einzeldaten. Insbesondere Bezahldienstleister, die eine Registrierung erfordern, erheben mehr Daten von den Nutzern. Auch die Anzahl übermittelter Daten durch die Händler variiert (zwischen zwei und 17).

Die Händler haben neben der Übermittlung obligatorischer Daten auch die Möglichkeit, weitere Daten des Nutzers optional an den elektronischen Bezahldienstleister zu übermitteln. Die Gesamtzahl übermittelter Daten liegt somit im Ermessen des jeweiligen Händlers. Über die reale Übermittlung von Daten an den Bezahldienstleister kann daher keine Aussage getroffen werden.

Die Händler übermitteln nicht nur Daten an den Bezahldienstleister: Nach erfolgreicher Bezahlung übermitteln die Bezahldienstleister ebenfalls Daten an die Händler. Diese sind zumeist identisch mit den ursprünglich übermittelten Daten. Bei Amazon Pay muss der Nutzer während der Bezahlung hierfür sein Einverständnis zur Übermittlung der Daten an den Händler erteilen. Erteilt er dieses nicht, wird der Zahlungsvorgang abgebrochen.

4 ANZAHL ÜBERMITTELTER NUTZERDATEN BEI REGISTRIERUNG UND BEZAHLUNG

	Amazon Pay	giropay	paydirekt	PayPal	Skrill	SOFORT Überweisung
Registrierung Anzahl eingegebener Daten durch Nutzer	4	–	11	9	8	–
Bezahlung Anzahl eingegebener Daten durch Nutzer	2	4	2	2	2	4
Bezahlung Anzahl übermittelter obligatorischer Daten von Shop	1	2	2	9	1	1
Bezahlung Anzahl übermittelter optionaler Daten von Shop	1	6	9	8	6	5

WELCHE TRACKING-DIENSTE VERWENDEN DIE BEZAHLDIENSTLEISTER?

Web-Tracking bezeichnet die Auswertung von Daten zur Verfolgung der Aktivitäten von Nutzern eines Web-Auftritts[65]. Die Einbindung dieser externen Dienste erlaubt es, das Verhalten eines Nutzers im World Wide Web über verschiedene Internetseiten hinweg in Echtzeit zu verfolgen[66]. Neben anonymisierten und pseudonymisierten Daten erhebt die Mehrzahl der Tracking-Dienste auch personenbeziehbare Daten[67]. Somit ermöglicht der Einsatz von Web-Tracking den Bezahldienstleistern, eine umfangreiche Datensammlung über ihre Nutzer aufzubauen. Neben dem allgemeinen Nutzungsverhalten auf einer Webseite können so gewonnene Informationen Aufschluss über Interessen und Konsumgewohnheiten von Nutzern geben und für gezielte Werbung verwendet werden[68].

Mit Hilfe der Browser-Erweiterung Ghostery (Version 6.3.2) erfolgte die Prüfung, ob und in welchem Rahmen die Bezahldienstleister auf ihren Webseiten Tracking-Dienste einsetzen. Auf Basis der dort bereitgestellten Datenbank aktueller Tracking-Tools und Werbenetzwerke wurden die von den Bezahldienstleistern eingesetzten Tracking-Dienste identifiziert und bezüglich der durch sie möglichen Datenerfassung aufgeschlüsselt[69].

Tabelle 5 fasst die mit Stand vom 08.06.2017 von den Bezahldienstleistern verwendeten Tracking-Dienste zusammen und verdeutlicht, welche Art der Datenerhebung den Bezahldienstleistern damit potentiell möglich ist.

Alle untersuchten Bezahldienstleister binden mindestens einen Tracking-Dienst im öffentlich zugänglichen Bereich ihrer Webseiten ein. Die Anzahl der eingesetzten Tracking-Dienste variiert: Insbesondere Skrill mit elf und PayPal mit sieben nutzen eine vergleichsweise hohe Anzahl externer Tracking-Dienste. Im Gegensatz dazu verwenden giropay und Amazon Pay jeweils zwei, paydirekt einen Tracking-Dienst. Zwei Bezahldienstleister setzen Tracking auch im privaten Bereich nach Login des Nutzers ein: paydirekt bindet hier den Tracking-Dienst Webtrekk ein, Skrill die Dienste Google Doubleclick, Google Tag Manager, Google Analytics und New Relic. Die Tracking-Dienste Google Tag Manager und New Relic geben gesichert personenbeziehbare Nutzerdaten an Dritte weiter.

Die Anzahl der eingesetzten Tracking-Dienste lässt nicht direkt auf die Quantität und Qualität der erhobenen Daten schließen. Jedoch ist die Mehrheit der genutzten Tracking-Dienste der Bezahldienstleister geeignet, personenbezogene bzw. personenbeziehbare Daten wie Namen, Adresse, Telefonnummer, E-Mail-Adresse oder **IP-Adresse** des Nutzers zu erheben. Der Großteil der eingebundenen Tracking-Dienste (16 von 22) erhebt personenbeziehbare Daten und elf dieser Dienste teilen diese auch mit Dritten.

FAZIT: NICHT JEDER BEZAHLDIENSTLEISTER FOLGT DER DATENSPARSAMKEIT

Im Ergebnis kann festgehalten werden, dass die untersuchten elektronischen Bezahldienstleister hinsichtlich der Einhaltung des Prinzips der Datensparsamkeit unterschiedliche Ansätze verfolgen. So variiert die Menge der durch die Bezahldienstleister erhobenen Nutzerdaten zwischen vier und 13 Einzeldaten. Auch der obligatorische und optionale Datenaustausch zwischen den Händlern und den Bezahldienstleistern unterscheidet sich: So können im Minimum zwei und im Maximum 17 Einzeldaten ausgetauscht werden. Insbesondere die Dienste ohne Registrierung wie giropay und SOFORT Überweisung erheben weniger Nutzerdaten. Paydirekt und PayPal erheben deutlich mehr Einzeldaten ihrer Nutzer. Amazon Pay erhebt vergleichsweise wenige Nutzerdaten. Einschränkend muss hier jedoch gesagt werden, dass der Bezahldienstleister Zugriff auf das Amazon-Nutzerkonto und somit insgesamt auf deutlich mehr Daten hat, als bei isolierter Betrachtung des Bezahldienstes.

65 Vgl. BSI (2014): M 2.488 Web-Tracking, online verfügbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02488.html, Stand 07.08.2017.

66 Vgl. Schneider et al. (2014): Web-Tracking-Report 2014, Fraunhofer-Institut für sichere Informationstechnologie, online verfügbar unter: https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Web_Tracking_Report_2014.pdf?_=1422365497, Stand 07.08.2017, S. 23.

67 Vgl. BSI (2014).

68 Vgl. Schneider et al. (2014), S. 23.

69 Einschränkend muss gesagt werden, dass es möglich ist, dass Tracking-Dienste von Ghostery nicht erkannt werden, wenn diese nicht in der Datenbank aufgeführt sind.

5 EINGESETZTE TRACKING-DIENSTE AUF DEN SEITEN DER BEZAHLDIENSTLEISTER

Anbieter	möglich erfasste Daten	Tracking-Dienste: Adobe Test&Target	Akamai Cookie Sync	AppNexus	Conversant	Dotomi	Facebook Connect	Facebook Custome Audience	Flashtalking	Google Analytics	Google Doubleclick	Google Tag Manager	Heap	Hotjar	LiveRamp	New Relic	Omniture	Optimizley	Piwik	Sovrn	ThreatMetrix	Webtrekk	yieldlab	Anzahl eingesetzter Tracker
Amazon Pay	anonymisiert	-	-	-	-	-	-	-	▲	-	-	-	-	-	-	-	▲	-	-	-	-	-	-	2
	pseudonymisiert	-	-	-	-	-	-	-	▲	-	-	-	-	-	-	-	▲	-	-	-	-	-	-	
	personenbeziehbar	-	-	-	-	-	-	-	○	-	-	-	-	-	-	-	▲	-	-	-	-	-	-	
giropay	anonymisiert	-	-	-	-	-	-	-	-	-	▲	-	-	-	-	-	-	-	○	-	-	-	-	2
	pseudonymisiert	-	-	-	-	-	-	-	-	-	▲	-	-	-	-	-	-	-	○	-	-	-	-	
	personenbeziehbar	-	-	-	-	-	-	-	-	-	▲	-	-	-	-	-	-	-	○	-	-	-	-	
paydirekt	anonymisiert	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	▲	-	1
	pseudonymisiert	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	▲	-	
	personenbeziehbar	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	○	-	
PayPal	anonymisiert	-	▲	▲	▲	▲	-	-	-	▲	▲	-	-	-	○	-	-	-	-	-	-	-	-	7
	pseudonymisiert	-	▲	▲	▲	▲	-	-	-	▲	▲	-	-	-	▲	-	-	-	-	-	-	-	-	
	personenbeziehbar	-	▲	▲	▲	▲	-	-	-	▲	▲	-	-	-	▲	-	-	-	-	-	-	-	-	
Skrill	anonymisiert	○	-	-	-	-	▲	▲	-	▲	▲	▲	-	▲	-	▲	▲	▲	-	-	▲	-	-	11
	pseudonymisiert	○	-	-	-	-	▲	▲	-	▲	▲	▲	-	▲	-	▲	▲	▲	-	-	▲	-	-	
	personenbeziehbar	○	-	-	-	-	▲	▲	-	▲	▲	▲	-	▲	-	▲	▲	▲	-	-	○	-	-	
SOFORT Überweisung	anonymisiert	-	-	-	-	-	-	-	-	-	▲	-	▲	-	-	-	-	-	-	▲	-	-	○	4
	pseudonymisiert	-	-	-	-	-	-	-	-	-	▲	-	▲	-	-	-	-	-	-	▲	-	-	○	
	personenbeziehbar	-	-	-	-	-	-	-	-	-	▲	-	▲	-	-	-	-	-	-	▲	-	-	○	

Legende: ○ = keine Angabe bei Ghostery, - = keine Erhebung durch Tracker, ▲ = Erhebung durch Tracker

Quelle: Ghostery

Stand: 08.06.2017

Die Untersuchung des Einsatzes von Tracking-Diensten zeigt deutliche Unterschiede zwischen den Bezahldienstleistern: Während paydirekt auf die Nutzung eines externen Dienstes setzt, bindet Skrill elf und PayPal sieben externe Tracking-Dienste auf dem öffentlich zugänglichen Web-Auftritt ein. Zwei der untersuchten Bezahldienstleister binden auch im privaten Bereich Tracking ein. Dies ist im Fall von paydirekt mit dem Dienst Webtrekk weniger kritisch zu bewerten, da dieser Dienst keine der erhobenen Nutzerdaten mit Dritten teilt und auch keine personenbeziehbaren Daten erhebt. Im Fall von Skrill geben die eingesetzten Dienste Google Tag Manager und New Relic auch personenbeziehbare Daten an Dritte weiter. Insgesamt gibt die Hälfte aller untersuchten Tracking-Dienste personenbeziehbare Daten an Dritte weiter.

4. TRANSPARENZ IM UMGANG MIT VERBRAUCHERDATEN

Das Recht auf informationelle Selbstbestimmung kann nur wirksam angewendet werden, wenn über die Datenverarbeitung transparent informiert wird. Der Verbraucher ist erst „Herr seiner Daten“, wenn er weiß, welche seiner Daten in welcher Art und Weise verarbeitet werden. So kann er entscheiden, ob er seine personenbezogenen Daten für den Nutzungsvorgang preisgeben möchte[70]. Obwohl der Transparenzgrundsatz wesentlicher Bestandteil des Datenschutzes ist, findet er weder im BDSG noch im TMG explizite Erwähnung. Er spiegelt sich jedoch in verschiedenen Regelungen, insbesondere zu den Informationspflichten[71] und den Auskunftsrechten[72], wider. Beide Teile – die Informationspflicht und das Auskunftsrecht – bilden die Säulen des datenschutzrechtlichen Transparenzgrundsatzes. Der besonderen Bedeutung der Transparenz wird künftig in der DSGVO Rechnung getragen: Diese wird dort explizit erwähnt. Nach Art 5 Abs. 1 lit. a DSGVO müssen personenbezogene Daten in „nachvollziehbarer Weise verarbeitet werden“. Hierzu werden den datenverarbeitenden Stellen künftig umfangreiche Informationspflichten auferlegt[73], um „eine faire und transparente Verarbeitung zu gewährleisten“.

WELCHE RECHTLICHEN ANFORDERUNGEN GELTEN FÜR DATENSCHUTZERKLÄRUNGEN?

Die Informationspflichten sind die erste Stufe für den transparenten Umgang mit personenbezogenen Daten. Die Bezahldienstleiser müssen den Verbraucher über die Datenverwendung informieren. Hierzu wird seitens dieser üblicherweise eine Datenschutzerklärung zur Verfügung gestellt. Über welche Inhalte in den Datenschutzerklärungen informiert werden muss, ergibt sich aus dem Gesetz. Welche Informationen zur Verfügung gestellt werden müssen, richtet sich im BDSG danach, ob die personenbezogenen Daten beim Betroffenen[74] oder ohne Kenntnis des Betroffenen[75] erhoben werden. Werden die Daten beim Betroffenen selbst erhoben, so muss über die Identität der verantwortlichen Stelle[76], die Zwecke der Datenverarbeitung sowie unter Umständen über die Kategorien[77] der Empfänger[78] informiert werden. Werden die Daten anderweitig erhoben, muss zudem über die Speicherung und die Art der Daten informiert werden. Nach den Unterrichtungspflichten des TMG muss der Verbraucher vor Beginn der Nutzung über Art, Umfang und Zweck der Erhebung und Verwendung personenbezogener Daten informiert werden. Zudem ist über die Verarbeitung seiner Daten in Staaten außerhalb des Anwendungsbereichs der Datenschutzrichtlinie zu unterrichten[79]. In der DSGVO wird danach unterschieden, ob die Daten beim Betroffenen selbst oder anderweitig erhoben wurden. Die Informationspflichten werden erweitert: So ist künftig über die Betroffenenrechte[80], die Speicherdauer, ein Profiling und das Beschwerderecht bei den Aufsichtsbehörden zu informieren[81].

Über die Art und Weise der Informationsvermittlung in den Datenschutzerklärungen finden sich wenige Anhaltspunkte im Gesetz. Generell gilt das Transparenzgebot. Darüber hinaus fordert § 13 Abs. 1 TMG, dass in „allgemein verständlicher Form“ zu unterrichten ist. Daraus ergeben sich bestimmte Anforderungen an den

70 Vgl. Jandt/Schaar/Schulz (2013), in: Roßnagel (Hg.), Beck‘scher Kommentar zum Recht der Telemediendienste, 1. Auflage, C.H.Beck, S. 222, Rn. 25.
71 Vgl. §§ 4 Abs. 3, 33 Abs. 1 BDSG; § 13 Abs. 1 TMG.
72 Vgl. § 34 BDSG; § 13 Abs. 8 TMG.
73 Vgl. Erwägungsgrund 60 DSGVO; Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) (2017): Datenschutzgrundverordnung, online verfügbar unter: https://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO6.pdf?__blob=publicationFile&v=24, Stand 08.08.2017, S. 56.
74 Vgl. § 4 Abs. 3 BDSG.
75 Vgl. § 33 Abs. 1 BDSG.
76 Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt; § 3 Abs. 7 BDSG.
77 Kategorien sind beispielweise: Bankinstitute, Versandhandelsunternehmen oder Marketing-Agenturen.
78 Werden die Daten an Dritte weitergegeben, muss über die Kategorien der Empfänger nur informiert werden, wenn der Betroffene mit der Übermittlung nicht rechnen muss.
79 Vgl. Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. EG Nr. L 281 S. 31).
80 Vgl. Kapitel 5: Recht auf Auskunft.
81 Vgl. Art 13 und 14 DSGVO.

sprachlichen Inhalt sowie an die äußere Gestaltung[82]. Der Verbraucher muss eine konkrete Vorstellung erhalten, wie seine Daten verwendet werden[83]. Er muss anhand der Formulierung erkennen können, worauf er sich einlässt, wenn er das Angebot der Bezahldienstleister nutzt. Ihm muss konkret bewusst werden, wer wann was über ihn weiß und er muss dadurch die Rechtmäßigkeit der Datenverarbeitung überprüfen können[84].

WIE WIRD IN DEN DATENSCHUTZ-ERKLÄRUNGEN INFORMIERT?

Alle sechs Bezahldienstleister verlinken Datenschutzerklärungen – Skrill jedoch nur auf eine Erklärung zur Nutzung seiner Webseite, nicht jedoch zur Bezahldienstleistung. Giropay verweist aufgrund seiner Funktionsweise auf die Datenschutzerklärung der genutzten Hausbank des Kunden. Somit stellt giropay keine gesonderte Datenschutzerklärung zum Bezahlvorgang zur Verfügung. Daher konnten nur vier der sechs Datenschutzerklärungen inhaltlich analysiert werden.

Die Bezahldienstleister informieren in unterschiedlicher Art und Weise. Alle informieren über die gesetzlichen Mindestinhalte, jedoch unterscheidet sich die Aussagekraft der Informationen innerhalb der Datenschutzerklärungen. Die inhaltliche Prüfung zeigt, dass in den Datenschutzerklärungen sprachlich mehrfach mit Formulierungen wie „zum Beispiel“ bzw. „z.B.“, „möglicherweise“ oder „unter anderem“ bzw. „u.a.“ gearbeitet wurde. So findet sich in der Datenschutzerklärung von Amazon Pay 31-mal die Aufzählung „z.B./zum Beispiel/beispielsweise“, 11-mal die Wortwendung „möglicherweise“ und siebenmal die Wortwendung „u.U./unter Umständen“. PayPal nutzt insgesamt 19-mal die Wortwendung „z.B./zum Beispiel/beispielsweise“, fünfmal „u.U./unter Umständen“, viermal die Formulierung „möglicherweise“ und dreimal die Aufzählung „u.a.“. Paydirekt verwendet in der Datenschutzerklärung 11-mal, SOFORT Überweisung sechsmal „z.B./zum Beispiel/beispielsweise“ zur Aufzählung. Diese Formulierungen ermöglichen es dem Verbraucher nicht, sich ein abschließendes Bild über den Umgang mit seinen Daten zu machen. Vielmehr lassen sie Spielraum für Unbestimmtheit.

Die Nutzung solcher offenen Wortwendungen zeigt sich besonders im Kontext der Datenkategorien und der Weitergabe an Dritte. Die Aufzählung, welche personenbezogene Daten erhoben werden, ist nur bei paydirekt abschließend. Die anderen drei Bezahldienstleister verwenden bei Aufzählung oben genannte Wortwendungen. Auch zur Art der weitergegebenen Daten sowie zu den Empfängern informieren die Dienstleister unterschiedlich: SOFORT Überweisung führt abschließend auf, welche Daten an welche Empfänger weitergegeben werden. In der Datenschutzerklärung heißt es hierzu: „Der Online-Anbieter erhält von uns die Bestätigung über die erfolgreiche Einstellung des Überweisungsauftrags zu Ihrer Bestellung. Diese umfasst nur die Daten aus dem Überweisungsformular (Name, Kontonummer, Bankleitzahl, Betreff, Überweisungsbetrag) sowie das Datum (mit Uhrzeit) und die vom Online-Anbieter gewählte Transaktionskennung (z.B. Auftragsnummer)“[85]. Paydirekt verwendet in der Datenschutzerklärung eine beispielhafte Aufzählung bezüglich der übermittelten Daten. Hier werden die Daten, die zur Durchführung des Dienstes an die Bank übermittelt werden, wie folgt bezeichnet: „Zahlungsdaten (z.B. Zahlungsbetrag, Angaben zum Zahlungsempfänger)“[86]. PayPal schlüsselt in einer 48-seitigen Liste[87] auf, welche Daten an welche Dritte weitergegeben werden. In der Datenschutzerklärung heißt es, dass es sich um „nicht ausschließliche Beispiele der Dritten“ handelt, denen gegenüber Kontoinformationen offengelegt werden. Amazon Pay führt bezüglich der Datenweitergabe an Drittanbieter von Dienstleistungen aus, dass „andere Firmen und Privatpersonen bei der Durchführung von Funktionen in unserem Auftrag ... Zugang zu persönlichen Daten, die zur Erfüllung ihrer Aufgaben benötigt werden“[88] haben.

82 Vgl. Müller-Broich (2012): Telemediengesetz, 1. Auflage, Nomos, § 13 Rn. 1.

83 Vgl. Jandt /Schaar/Schulz (2013), S. 224 Rn. 37.

84 Vgl. Nink/Spindler (2015), in: Spindler/Schuster (Hg.): Recht der elektronischen Medien, 3. Auflage, C.H.Beck, TMG § 13, Rn. 3.

85 SOFORT GmbH (2015): Datenschutzhinweise, online verfügbar unter: https://documents.sofort.com/sue/datenschutzhinweise_ch, Stand 22.07.2016.

86 paydirekt (2016): Hinweise zum Datenschutz, online verfügbar unter: https://www.paydirekt.de/agb/index.html, Stand 27.07.2016.

87 PayPal (2017b): PayPal-Datenschutzgrundsätze, online verfügbar unter: https://www.paypal.com/de/webapps/mpp/ua/privacy-full?locale.x=de_DE, Stand 01.07.2017.

88 Amazon Pay (2013): Datenschutzbestimmungen, online verfügbar unter: https://pay.amazon.com/de/help/201751600, Stand 25.07.2016.

Im Gegensatz dazu geben alle Bezahldienstleister an, dass sie personenbezogene Daten erheben. Auch der Fakt, dass die Daten an Dritte weitergegeben werden, wird unmissverständlich in den Datenschutzerklärungen der Bezahldienstleister kommuniziert.

ZU WELCHEN ZWECKEN WERDEN DIE VERBRAUCHERDATEN VERWENDET?

Mehr als ein Drittel der befragten Nutzer von Bezahldienstleistern geht davon aus, dass seine Daten für Werbezwecke verarbeitet werden[89]. Gleichzeitig gibt jeder Dritte an, den Bezahldienstleister nicht mehr nutzen zu wollen, wenn der Anbieter die personenbezogenen Daten für die Erstellung eines Nutzungsprofils verwendet oder an Dritte zum Zwecke der personalisierten Werbung weitergibt[90]. Somit ist es die Verwendung persönlicher Daten über den eigentlichen Vertragszweck hinaus, welche Verbraucher ablehnen.

Vor diesem Hintergrund werden die Datenschutzerklärungen der Bezahldienstleister auf Angaben über den Zweck der Datenverwendung ausgewertet. Die Datenverwendung umfasst die Nutzung für eigene Zwecke als auch die Weitergabe an Dritte für eigene und Zwecke Dritter.

Berücksichtigt werden vertragliche Zwecke, Sicherheits- und Marketingzwecke sowie die Verwendung der Daten für das Erstellen eines Nutzungsprofils. Vertragliche Zwecke werden dabei als solche Zwecke verstanden, die zur Durchführung des Vertrages notwendig sind; Sicherheitszwecke als diejenigen, bei denen Daten beispielsweise verwendet werden, um Missbrauch oder Identitätsdiebstahl vorzubeugen. Die Verwendung zu Marketingzwecken umfasst unter anderem die Eigen- und Drittwerbung sowie die Nutzung der Daten zur Optimierung des eigenen Angebots. Nutzungsprofile geben Aufschluss über die Nutzung des Angebots durch den Kunden[91]. Für die Auswertung mussten Nutzungsprofile in den Datenschutzerklärungen explizit als solche bezeichnet werden oder ein Verweis auf personalisierte Angebote erfolgen.

Tabelle 6 schlüsselt auf, für welche Zwecke personenbezogene Daten durch den Bezahldienstleister laut deren Datenschutzerklärungen verwendet werden.

Amazon Pay und PayPal nutzen die erhobenen Daten nach eigenen Angaben außer zur Erfüllung der Vertrags- und Sicherheitszwecke auch für Marketingzwecke und für die Bereitstellung von personalisierten Angeboten. Paydirekt und SOFORT Überweisung nutzen sie laut ihrer untersuchten Datenschutzerklärungen ausschließlich für Vertragszwecke und Sicherheitsaspekte.

6 ZWECK DER DATENVERWENDUNG

Zweck der Datenverwendung	Amazon Pay	paydirekt	PayPal	SOFORT Überweisung
Vertragliche Zwecke	ja	ja	ja	ja
Sicherheitszwecke	ja	ja	ja	ja
Marketingzwecke	ja	nein	ja	nein
Nutzungsprofile	ja	nein	ja	nein

89 Vgl. Dautzenberg et al. (2017a), S. 32.
90 Vgl. ebenda.
91 Vgl. Habel/Müller (2017), in: Forgó/Helfrich/Schneider (Hg.): Betrieblicher Datenschutz, 2. Auflage, C.H.Beck, Teil X, Kapitel 3, Rn. 11.

WIE VERSTÄNDLICH SIND DATENSCHUTZERKLÄRUNGEN?

Angaben zum Datenschutz stellen oft große Herausforderungen an den Leser, da sie aufgrund der Vielschichtigkeit des zu beschreibenden Sachverhalts sehr umfangreich sein können und häufig komplexe Formulierungen verwenden[92]. Jeder dritte Leser (35 Prozent) von Datenschutzerklärungen empfindet diese als „nicht hilfreich“[93]. Das verdeutlicht die Problematik, dass – selbst wenn Bezahldienstleister rechtskonform und vollständig über den Umgang mit Nutzerdaten unterrichten – nicht sichergestellt ist, dass Nutzer über den Umgang mit ihren Daten tatsächlich informiert sind. Datenschutzerklärungen sollten daher so verständlich wie möglich geschrieben sein. Die Verständlichkeit der Datenschutzerklärungen bildet die Grundlage, um sich deren Inhalte und Informationen zu erschließen. Nachfolgend werden die Datenschutzerklärungen der elektronischen Bezahldienstleister auf ihre formale Verständlichkeit hin geprüft. Alle vier oben genannten Datenschutzerklärungen (vgl. Kapitel 4) wurden einer Verständlichkeitsanalyse mit TextLab unterzogen. Die Ergebnisse werden nachfolgend dargestellt.

Die Datenschutzerklärung von Amazon Pay[94] umfasst insgesamt 3.670 Wörter in 169 Sätzen. Im Detail zeigt sich, dass nahezu die Hälfte der Sätze (46 Prozent) der Datenschutzerklärung deutlich länger als 20 Wörter ist. Der längste Satz des Dokuments umfasst 95 Wörter. Weiterhin kann ein vergleichsweise geringer Anteil an Nominalsätzen (13 Prozent) und Füllwörtern (1 Prozent) gefunden werden. Der niedrige Anteil von Füllwörtern indiziert jedoch eine sehr hohe Informationsdichte im Text. Die Datenschutzerklärung von Amazon Pay kann gemessen am „Hohenheimer Verständlichkeitsindex“ (HIX) mit einem Wert von 4,0 als sehr schwer verständlich eingeordnet werden. Der Index ordnet basierend auf oben genannten Text-Kennzahlen die Verständlichkeit von Texten auf einer Skala von 0 „überhaupt nicht verständlich“ bis 20 „sehr leicht verständlich“ ein[95]. Die Datenschutzerklärung von paydirekt[96] umfasst 1.549 Wörter in 89 Sätzen. Ein Viertel der Sätze (24 Prozent) enthält mehr als 20 Wörter. Paydirekt verwendet in 29 Prozent der Sätze Passivkonstruktionen, die als schwer verständlich zu bewerten sind. Die Datenschutzerklärung ist insgesamt mit einem HIX-Wert von 6,6 als schwer verständlich einzuordnen. Die Datenschutzerklärung von PayPal[97] umfasst insgesamt 5.985 Wörter in 273 Sätzen. Fast jeder zweite Satz (45 Prozent) besteht aus mindestens 20 Wörtern – teils sogar deutlich mehr. Der längste Satz beinhaltet 95 Wörter. Trotz sparsamer Verwendung von langen Wörtern (3 Prozent) oder Füllwörtern (0,4 Prozent) kann eine solche Länge der Sätze die Verständlichkeit des Textes stark behindern. Die Datenschutzerklärung von PayPal ist mit einem HIX-Wert von 2,5 als formal unverständlich zu werten. Die Datenschutzerklärung von SOFORT Überweisung[98] besteht aus 906 Wörtern in 54 Sätzen. Der Anteil langer Sätze im Fließtext liegt deutlich über den Empfehlungen für einen verständlichen Text: Neben knappen Aufzählungen umfasst jeder dritte Satz (37 Prozent) der Datenschutzerklärungen des Bezahldienstleisters mehr als 20 Wörter. Ein Viertel der Sätze (26 Prozent) ist zudem in potentiell schlechter verständlichen Passivkonstruktionen geschrieben. Die Datenschutzerklärung von SOFORT Überweisung ist im Gesamten mit einem HIX-Wert von 7,1 als schwer verständlich zu werten.

Tabelle 7 (Seite 30) fasst die Einordnung der untersuchten Datenschutzerklärungen hinsichtlich ihrer formalen Verständlichkeit zusammen.

Insgesamt kann die formale Verständlichkeit der untersuchten Datenschutzerklärungen als unverständlich bzw. schwer verständlich gewertet werden. Der Umfang der Datenschutzerklärungen variiert deutlich: So umfasst die kürzeste Datenschutzerklärung 906 Wörter und die Längste 5.985 Wörter. Der Anteil langer Sätze bei Fachtexten sollte einen Zielwert von 10 Prozent nicht überschreiten, um die Komplexität des geschriebenen Textes zu reduzieren. Alle der vorliegenden Datenschutzerklärungen überschreiten diesen Zielwert deutlich. Die Problematik der formalen Verständlichkeit wird am Beispiel des jeweils längsten Satzes aus den vorliegenden Datenschutzerklärungen illustriert (vgl. hierzu **Abbildung 8**, Seite 31).

92 Vgl. McDonald et al. (2009): A Comparative Study of Online Privacy Policies and Formats, in: Privacy Enhancing Technologies. PETS 2009. Lecture Notes in Computer Science. Jg. 5672, S. 3.
93 Vgl. Dautzenberg et al. (2017a), S. 32.
94 Mit Stand vom 25.07.2016.
95 Vgl. hierzu: Verständlichkeitsanalyse zur Transparenz im Umgang mit Verbraucherdaten und Recht auf Auskunft im Kapitel 1 "Methodik"
96 Mit Stand vom 27.07.2016.
97 Mit Stand vom 28.07.2016.
98 Mit Stand vom 22.07.2016.

7 FORMALE TEXTEIGENSCHAFTEN DER DATENSCHUTZERKLÄRUNGEN

Analyse der Datenschutzerklärungen	Zielwert	Amazon Pay	paydirekt	PayPal	SOFORT Überweisung
Hohenheimer Index (HIX)	12,0	4,0	6,6	2,5	7,1
Länge des längsten Satzes (in Wörtern)		95	46	95	33
Anzahl der Sätze		169	89	273	54
Anzahl der Wörter		3.670	1.549	5.985	906
Anteil Sätze >20 Wörtern	10 %	46 %	35 %	45 %	37 %
Anteil Sätze im Passiv	15 %	15 %	23 %	14 %	26 %
Anteil Sätze im Nominalstil	20 %	13 %	17 %	16 %	7 %
Anteil Füllwörter	1 %	1 %	0,5 %	0,4 %	1,2 %

Legende: Interpretation HIX: 0 (formal unverständlich) bis 20 (formal sehr verständlich); Dokumentenart: Fachtext

FAZIT: DATENSCHUTZERKLÄRUNGEN LASSEN INTERPRETATIONSSPIELRAUM UND SIND SCHWER VERSTÄNDLICH

Der Informationspflicht über die Datenverwendung kommen die elektronischen Bezahldienstleister durch die gängige Praxis mit Hilfe von Datenschutzerklärungen nach. In der DSGVO werden die Informationspflichten erweitert: Informationen müssen künftig über Betroffenenrechte, Speicherdauer, Profiling und Beschwerderecht bei den Aufsichtsbehörden gegeben werden. Die Art und Weise der Informationsvermittlung unterliegt dem Transparenzgebot und muss in „allgemein verständlicher Form“[99] erfolgen. Der Verbraucher muss damit anhand der Formulierung erkennen können, worauf er sich einlässt, wenn er das Angebot eines Bezahldienstleisters in Anspruch nimmt.

Die Ergebnisse zeigen: Skrill stellt eine Datenschutzerklärung zur Nutzung seiner Internetseite zur Verfügung, nicht aber zur Bezahldienstleistung. Alle untersuchten Datenschutzerklärungen informieren über gesetzliche Mindestinhalte. Die Aussagekraft der Informationen innerhalb der Datenschutzerklärungen variieren erheblich: Durch Verwendung sprachlicher Formulierungen wie „zum Beispiel“ werden Aufzählungen zu Angaben erhobener personenbezogener Daten nicht abschließend benannt. Dieses Vorgehen wählen Amazon Pay, PayPal und SOFORT Überweisung. Auch bei Angaben zur Art der weitergegebenen Daten sowie zu den jeweiligen Empfängern gibt nicht jeder Bezahldienstleister abschließende Informationen. Häufig genutzte Wortwendungen wie „zum Beispiel“ „möglicherweise“ und „unter anderem“ lassen Zweifel entstehen, ob der Verbraucher anhand dieser Formulierungen tatsächlich in die Lage versetzt wird, zu erkennen, worauf er sich bei Nutzung des Dienstes konkret einlässt. Positiv fällt auf, dass alle Bezahldienstleister konkrete Angaben – ohne Verwendung oben genannter Wortwendungen – dazu machen, dass sie personenbezogene Daten erheben und an Dritte weitergeben.

Die Bezahldienstleister Amazon Pay und PayPal nutzen die erhobenen Daten neben der Erfüllung der Vertrags- und Sicherheitszwecke auch für Marketingzwecke und die Bereitstellung personalisierter Angebote. Paydirekt und SOFORT Überweisung verzichten laut ihrer Datenschutzerklärungen darauf. Der Nutzer kann keinen akti-

99 Vgl. TMG § 13 Abs. 1.

8 BEISPIELSÄTZE AUS DEN UNTERSUCHTEN DATENSCHUTZERKLÄRUNGEN

Längster Satz Datenschutzerklärung paydirekt (46 Wörter):
„Im Zusammenhang mit einer vom Teilnehmer beantragten Erstattung im Konfliktfall (Ziff. 14 der Bedingungen für Zahlungen mittels paydirekt) erhebt die paydirekt GmbH die vom Teilnehmer übermittelten Daten (z.B. Name des Händlers, Artikelbezeichnung, Vor- und Nachname des Teilnehmers, Bestelldatum, Liefer- und Rechnungsadresse, Gesamtpreis der Bestellung, Nachrichten des Händlers).“

Längster Satz Datenschutzerklärung Amazon Pay (95 Wörter):
„Weitere Beispiele für Situationen, in denen Sie uns Daten mitteilen, sind u.a.: die Durchführung von Bestellungen unter Nutzung unserer Services, auch über Websites Dritter, die unsere Services nutzen, die Eingabe von Daten im Menüpunkt "Ihr Konto" (es kann auch sein, dass Sie über mehr als ein Konto verfügen, falls Sie bei der Nutzung unserer Services mehr als eine E-Mail-Adresse verwendet haben) bei Kommunikation mit uns per Telefon, E-Mail oder anderweitig, dem Ausfüllen eines Fragebogens oder eines Teilnahmeformulars für ein Preisausschreiben und die Nutzung anderer Benachrichtigungsdienste, wie sie z.B. für Benachrichtigungen über Bestellungen zur Verfügung stehen.“

Längster Satz Datenschutzerklärung PayPal (95 Wörter):
„Wenn ein registrierter Benutzer der PayPal-Services versucht, eine Transaktion mit einer Person, die kein registrierter Benutzer der PayPal-Services ist, auszuführen (zum Beispiel, indem er der Person eine Zahlung oder einen anderen Vorteil sendet oder eine Zahlung von dieser Person anfordert), bewahren wir zum Vorteil des registrierten Benutzers der PayPal-Services, der versucht, die andere Partei zu kontaktieren, die Daten auf, die der registrierte Benutzer der PayPal-Services an uns übermittelt, z.B. die E-Mail-Adresse, Telefonnummer, und/oder den Namen der anderen Partei, damit der registrierte Benutzer der PayPal-Services eine vollständige Aufzeichnung seiner Transaktionen erhält, auch nicht abgeschlossener Transaktionen.“

Längster Satz Datenschutzerklärung SOFORT Überweisung (33 Wörter):
„Sofern uns bekannt wird, dass trotz unserer positiven Prüfung eine SOFORT Überweisung nicht beim Zahlungsempfänger eingegangen ist (z.B. weil ein Händler uns dies nachträglich meldet), informieren wir den betroffenen Kunden beim nächsten Überweisungsversuch hierüber.“

ven Einfluss darauf nehmen, zu welchen Zwecken seine Daten verwendet werden.

Die formale Verständlichkeit der untersuchten Datenschutzerklärungen wird als unverständlich oder schwer verständlich bewertet. Die Textlängen der Datenschutzerklärungen variieren stark. So benötigt ein Leser bei einer angenommenen Lesegeschwindigkeit von 250 Worten pro Minute[100] für das Lesen der Datenschutzerklärung von PayPal 24 Minuten, im Fall der kürzesten Datenschutzerklärung von SOFORT Überweisung nur knapp vier Minuten. Zum Lesen der Datenschutzerklärung von paydirekt müssen gut sechs Minuten und von Amazon Pay 15 Minuten aufgewendet werden. Bei allen untersuchten Datenschutzerklärungen erschweren lange Sätze dem Leser die Verständlichkeit. Die Datenschutzerklärungen von paydirekt und SOFORT Überweisung nutzen nahezu jeweils in rund einem Viertel der Sätze Passivkonstruktionen, welche eine zusätzliche, unnötige Distanz zum Leser[101] schaffen.

100 Vgl. McDonald/Cranor (2008): The Cost of Reading Privacy Policies, online verfügbar unter: http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf, Stand 07.08.2017, S. 10.

101 Vgl. Brettschneider (2014), S. 38.

5. RECHT AUF AUSKUNFT

Um die Transparenz der Datenverwendung zu ermöglichen, haben Verbraucher ein Recht auf Auskunft[102]. Vollständige Transparenz kann nur dann hergestellt werden, wenn der Verbraucher von dem Bezahldienstleister validierte Informationen über die Verwendung seiner Daten erhält[103]. Erst diese Informationen versetzen den Verbraucher in die Lage über die weitere Geltendmachung seiner Rechte zu entscheiden und sind daher wesentliche Voraussetzung zum Selbstdatenschutz[104]. Die Betroffenenrechte des Verbrauchers beinhalten insbesondere das Recht auf Auskunft sowie die Berichtigung und Löschung von Daten.

WAS BEINHALTET DAS RECHT AUF AUSKUNFT?

Der elektronische Bezahldienstleister ist nach § 34 BDSG verpflichtet[105], den Verbraucher kostenfrei[106] über die Verwendung seiner Daten zu informieren. Der Auskunftsanspruch erstreckt sich auf Informationen über die zu einer Person gespeicherten Daten, die Herkunft dieser Daten und den Zweck der Speicherung. Werden die Daten an Dritte weitergegeben, müssen die Empfänger oder die Kategorien der Empfänger[107] benannt werden[108]. Die Auskunft ist grundsätzlich in Textform[109] zu erteilen. Ab Mai 2018 werden im Rahmen der DSGVO die Auskunftspflichten umfangreicher und erfassen dann unter anderem gemäß Art 15 Abs. 1 und 2 DSGVO auch Informationen zu den Verarbeitungszwecken, der geplanten Speicherdauer sowie über das Bestehen einer automatisierten Entscheidungsfindung, einschließlich Profiling. Darüber hinaus ist der Antragssteller im Auskunftsschreiben dann auch über sein Recht auf Berichtigung und Löschung sowie das Recht auf Beschwerde bei den Aufsichtsbehörden zu informieren.

Voraussetzung für die Auskunft ist ein entsprechender Antrag des Verbrauchers. Die Form des Antrags ist nicht vorgeschrieben und muss keine Begründung enthalten. Der Antrag kann mündlich oder schriftlich erfolgen. Die angefragten Unternehmen müssen aus Haftungsgründen allerdings sicherstellen, dass die Auskunft tatsächlich nur gegenüber der betroffenen Person erfolgt. Um die Identität des Verbrauchers zu prüfen, kann das Unternehmen daher verlangen, dass der Auskunftsanspruch schriftlich und, falls notwendig, per Post gesendet wird. Zur Identifizierung der Person wird teilweise die Vorlage oder Kopie des Personalausweises seitens des Bezahldienstleisters verlangt. Inwieweit der Besitzer des Personalausweises überhaupt eine solche Kopie anfertigen und herausgegeben darf, ist dem Personalausweisgesetz nicht zu entnehmen. Die Intersoft Consulting AG hat deswegen im März 2016 eine Anfrage an das Bundesministerium des Inneren (BMI) gestellt, ob ein generelles Kopierverbot des Ausweises besteht[110]. Laut dem BMI besteht ein solches Kopierverbot nicht, allerdings sollen Daten, welche nicht zur Identifizierung notwendig sind, auf der Kopie geschwärzt werden. Dies gelte vor allem für die auf dem Ausweis aufgedruckte Zugangs- und Seriennummer. Im Rahmen der Untersuchung wurde bezüglich der Schwärzung der Kopie eine erneute Anfrage an das BMI gestellt. In dem Antwortschreiben führt das BMI aus: „Daten, die nicht zu Identifizierung benötigt werden, sollten vom Dokumenteninhaber auf der Kopie unkenntlich gemacht werden, z. B. durch Schwärzung. Laut BMI ist darüber hinaus der Ausweisinhaber auf die Möglichkeit und Notwendigkeit der Schwärzung hinzuweisen[111]. Die Bundesbeauftrag-

102 Das Recht auf Auskunft lautet nach BDSG § 34 „Auskunft an den Betroffenen“. Betroffene im Sinne des BDSG sind natürliche Personen, deren personenbezogene oder personenbeziehbare Daten verarbeitet werden. Der Begriff des „Betroffenen“ umfasst also mehr Personen als der Begriff des „Verbrauchers“. Im Nachfolgenden werden die Begriffe Verbraucher und Betroffener im Sinne des BDSG synonym verwendet. So unter anderem nach § 34 Abs. 7 BDSG, z.B. wenn die Daten zu eigenen Zwecken gespeichert sind und ohnehin aus allgemein zugänglichen Quellen entnommen sind.

103 Vgl. §§ 33ff. BDSG.

104 Vgl. Worms (2017), in: Wolff/Brink (Hg.), BeckOK Datenschutzrecht, 20. Auflage, C.H.Beck, § 19 BDSG.

105 Unter bestimmten Voraussetzungen besteht keine Pflicht zur Auskunftserteilung. So unter anderem nach § 34 Abs. 7 BDSG.

106 In anderen Ländern kann für die Auskunft einer Gebühr verlangt werden.

107 Kategorien sind beispielweise: Bankinstitute, Versandhandelsunternehmen oder Marketing-Agenturen.

108 Nach § 34 Abs. 4 BDSG umfasst die Auskunft bei bestimmten Unternehmen auch die Scorewerte.

109 Vgl. § 126 b BGB.

110 Vgl. Mommers (2012): Nicht bemerkt?! Personalausweis kopieren verboten!, online verfügbar unter: https://www.datenschutzbeauftragter-info.de/nicht-bemerkt-personalausweis-kopieren-verboten/, Stand 07.08.2017.

111 Vgl. BMI: Ausweiskopien sind mit Einverständnis erlaubt, online verfügbar unter: http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Der-Personalausweis/Ausweis_kopieren/ausweis_kopieren_node.html, Stand 20.09.2017.

te für den Datenschutz und die Informationssicherheit (BfDI) weist darauf hin, dass für die Identifizierung nur folgende Angaben benötigt werden: "Name, Anschrift, Geburtsdatum und Gültigkeitsdauer des Dokuments“.

Nachfolgend wird dargestellt, ob betroffenen Verbrauchern das Recht auf Auskunft seitens der untersuchten Bezahldienstleister gewährt wird und in welcher Weise und Zeit die elektronischen Bezahldienstleister auf einen entsprechenden Antrag auf Auskunft reagieren. Insbesondere wird auch auf die Inhalte und die Verständlichkeit der Auskunftsschreiben eingegangen.

Im Fall der Untersuchung versendeten jeweils die Testkäufer ein standardisiertes Schreiben mit der Bitte um Auskunft per E-Mail[112].

WIE REAGIEREN BEZAHLDIENSTLEISTER AUF DAS AUSKUNFTSVERLANGEN?

Insgesamt kann konstatiert werden, dass die untersuchten Bezahldienstleister auf das Auskunftsersuchen in deutlich unterschiedlicher Schnelligkeit und Verfahrensweise reagieren. **Tabelle 9** fasst den Auskunftsprozess für alle elektronischen Bezahldienstleister zusammen.

9 ÜBERBLICK DES AUSKUNFTSPROZESSES

	Amazon Pay	giropay	paydirekt	PayPal	Skrill	SOFORT Überweisung
Reaktion Auskunfts-verlangen	standardi-sierte Kunden-E-Mail ohne Bezugnahme	keine Reaktion	Auskunfts-schreiben	standardi-sierte Kunden-E-Mail ohne Bezugnahme	keine Reaktion	E-Mail mit Bitte um Identitäts-nachweis
Reaktion 1. Nachfrage	E-Mail mit Verweis auf Hilfeseiten	standardi-sierte Kunden-E-Mail ohne Bezugnahme		E-Mail mit Bitte um Iden-titätsnachweis	keine Reaktion	E-Mail mit Sende-mitteilung zur Auskunft
Reaktion 2. Nachfrage	E-Mail mit allgemeinen Informationen zu Kunden-daten	Auskunfts-schreiben		E-Mail mit Bitte um un-geschwärzten Identitäts-nachweis	keine Reaktion	Auskunfts-schreiben
Reaktion 3. Nachfrage	Auskunfts-schreiben und CD			geschwärzter Identitäts-nachweis wird nicht akzeptiert	E-Mail mit Aufforderung von 10 £ und Ausweiskopie	
Auskunft erhalten?	ja	ja	ja	Auskunfts-ersuchen abgebrochen	Auskunfts-ersuchen abgebrochen	ja
Dauer in Tagen	62	14	2	21	50	2

112 Vgl. hierzu: Inhaltliche Analyse der Transparenz im Umgang mit Verbraucherdaten und dem Recht auf Auskunft im Kapitel 1 "Methodik"

Paydirekt übersandte die Auskunft ohne weitere Kundenkommunikation direkt auf das Auskunftsverlangen hin innerhalb der Dauer von zwei Tagen per Brief an die Privatadresse. Ein Identitätsnachweis zum Beispiel über eine geschwärzte Kopie des Personalausweises wurde nicht gefordert. Das Auskunftsschreiben von SOFORT Überweisung erreichte den Betreffenden ebenfalls innerhalb von zwei Tagen. Hier wurde im Vorfeld um einen Identitätsnachweis der ersuchenden Person in Form einer geschwärzten Kopie des Personalausweises gebeten. Die Übersendung der Auskunft erfolgte in Form eines Einwurfeinschreibens. Amazon Pay reagierte auf das Auskunftsersuchen zunächst in Form einer standardisierten Kundendienst-E-Mail ohne Bezug auf das Anliegen. Auf erneute Rückfrage versendete der Dienstleister eine E-Mail mit Verweis auf allgemeine Hilfeseiten der Webseite von Amazon. Auf weitere Nachfrage erreichte den Betroffenen eine E-Mail mit allgemeinen Informationen zur Datenauskunft und einem Verweis auf die geltende Datenschutzrichtlinie des Dienstleisters. Eine dann erfolgte schriftliche Anfrage auf Auskunft führte nach 14 Tagen erfolgreich zur Zustellung der Datenauskunft. Der Gesamtzeitraum zwischen der ersten Anfrage und dem Erhalt der Auskunft betrug 62 Tage. Giropay reagierte auf das Auskunftsersuchen zunächst nicht. Bei wiederholter Anfrage sendete der Dienstleister eine standardisierte Kunden-E-Mail ohne Bezug zum Anliegen. Nur wenige Stunden später erfolgte dann per E-Mail das Auskunftsschreiben. Der Gesamtzeitraum zwischen erster Anfrage und Erhalt des Schreibens betrug 14 Tage. PayPal antwortete in erster Reaktion mit einer standardisierten Kundendienst-E-Mail ohne Bezug zum Anliegen. In der nächsten Anfrage erbat PayPal einen Identitätsnachweis. Zur Identifizierung erfolgte die Übersendung eines geschwärzten Personalausweises[113]. Da PayPal jedoch nur eine Kopie akzeptierte, die „Foto, Angaben zu Größe und ähnliches“[114] geschwärzt darstellen, jedoch explizit eine ungeschwärzte Identifikationsnummer verlangte, wurde das Auskunftsersuchen nach 21 Tagen abgebrochen. Skrill reagierte auf das Auskunftsersuchen der ersten zwei Anfragen nicht. Bei dritter Nachfrage bat der Bezahldienstleister in einer englischsprachigen Mail um eine Ausweiskopie bei gleichzeitiger Übersendung eines Schecks in Höhe von 10 £[115], woraufhin das Ersuchen abgebrochen wurde. Der Gesamtzeitraum bis zum Abbruch betrug insgesamt 50 Tage.

WIE WIRD IN DEN AUSKUNFTSSCHREIBEN INFORMIERT?

Insgesamt lagen für die inhaltliche Auswertung vier Auskunftsschreiben der elektronischen Bezahldienstleister vor. Explizit gefragt wurde im Anschreiben nach den gespeicherten Daten, dem Zweck der Datenerhebung, der Herkunft, der Datenübermittlung und Empfänger der Daten, nach der Anlegung eines Nutzungsprofils und nach dem Scorewert. Giropay verweist in seinem Schreiben darauf, „dass die Bezahlung mit giropay im sicheren Online-Banking Ihrer Sparkasse oder Bank stattfindet. Dadurch ist garantiert, dass sensible und persönliche Daten ausschließlich zwischen Ihnen und Ihrer Sparkasse/Bank ausgetauscht werden. Kein Dritter erhält Einblick in Ihre persönlichen Konto- und Umsatzinformationen“[116]. Daher wird giropay nachfolgend nicht in die Auswertung der Auskunftsschreiben einbezogen.

Tabelle 10 stellt die Antwortkategorien der drei weiteren Bezahldienstleister zu den jeweiligen Fragen dar.

Amazon Pay nimmt in seinem Auskunftsschreiben nicht Bezug auf Amazon Pay sondern auf das Amazon-Kundenkonto allgemein. Auf die Fragen zu Nutzungsprofil und Scorewert gibt der Dienstleister keine Antwort. Paydirekt und SOFORT Überweisung nehmen in ihren Schreiben auf alle Fragen Bezug.

113 Bei der Schwärzung wurde sich an die oben genannte Anforderung der Bundesbeauftragten für den Datenschutz und die Informationssicherheit gehalten.

114 E-Mail vom PayPal vom 25.08.2016.

115 In Großbritannien kann eine Gebühr von maximal 10 £ für das Auskunftsbegehren verlangt werden. Vgl. Information Commissioner's Office (ico) (2017): Can I charge a fee for dealing with a subject access request?, online verfügbar unter: https://ico.org.uk/for-organisations/guide-to-data-protection/principle-6-rights/subject-access-request/, Stand: 01.07.2017.

116 Auskunftsschreiben von giropay vom 04.10.2016.

10 ANGABEN IN DEN AUSKUNFTSSCHREIBEN

	Amazon Pay	paydirekt	SOFORT Überweisung
Angaben zu gespeicherten Daten	Name, E-Mail-Adresse, Adressen, Telefonnummer; Zahlungsarten, Bestellungen, Merklisten, Gutscheine, Rücksendungen, Garantieansprüche; Wunschzettel, Abonnements, Cloud Drive Kontodetails, Cloud Drive Storage Details, Music Storage Details, Kindle; Digitale Bibliothek, AIV Events, Trade-Ins	Stammdaten (Kundenname, Benutzername, Geburtsdatum, E-Mail-Adresse, Telefonnummer), Kontoeröffnung, Sicherheitsverfahren, Zahlungsinformationen, Adressen (Postanschrift, Versandanschrift), Transaktionsdaten, Zahlungsdetails	Name, Zahlungsinformationen, Transaktionsdaten: Betrag, Datum, Empfänger
Zweck der Datenerhebung	✓	✓	✓
Datenherkunft	✓	✓	✓
Datenübermittlung und Empfänger der Daten	✓	✓	✓
Nutzungsprofil	✗	✓	✓
Scorewert	✗	✓	✓

Legende: ✓ = Angaben, ✗ = keine Angaben.

WIE VERSTÄNDLICH SIND DIE AUSKUNFTSSCHREIBEN?

Das Auskunftsschreiben von Amazon Pay umfasst insgesamt 1.112 Wörter in 61 Sätzen. Hier ist mit 36 Prozent insbesondere der Anteil langer Sätze deutlich über dem Zielwert eines verständlichen Schreibens. Verbunden mit einen erhöhten Anteil an Passivsätzen (20 Prozent) sowie Füllwörtern (1,6 Prozent) liegt die Auskunft von Amazon Pay damit im formal unverständlichen Bereich (HIX-Wert = 5,4). Die Datenauskunft von paydirekt ist dagegen als sehr verständlich zu werten (HIX-Wert = 16,3). Insgesamt umfasst die Auskunft 161 Wörter in 19 Sätzen. Das Auskunftsschreiben von SOFORT Überweisung umfasst 222 Wörter in 14 Sätzen. Die formale Verständlichkeit ist durch einen hohen Anteil an Passivkonstruktionen (36 Prozent) und Nominalformulierungen (21 Prozent) als schwer verständlich zu werten (HIX-Wert = 9,9).

Tabelle 11 (siehe Seite 36) fasst die Einordnung der untersuchten Datenschutzerklärungen hinsichtlich ihrer formalen Verständlichkeit zusammen.

11 FORMALE TEXTEIGENSCHAFTEN DER AUSKUNFTSSCHREIBEN

Verständlichkeitsparameter	Zielwert	Amazon Pay	paydirekt	SOFORT Überweisung
Hohenheimer Index (HIX)	14,0	5,4	16,3	9,9
Länge des längsten Satzes (in Wörtern)		58	18	33
Anzahl der Sätze		61	19	14
Anzahl der Wörter		1.112	161	222
Anteil Sätze >20 Wörtern	3 %	36 %	0 %	14 %
Anteil Sätze im Passiv	10 %	20 %	5 %	36 %
Anteil Sätze im Nominalstil	20 %	7 %	5 %	21 %
Anteil Füllwörter	1 %	1,6 %	0,0 %	1,4 %

Legende: Interpretation HIX: 0 (formal unverständlich) bis 20 (formal sehr verständlich); Dokumentenart: Brief

FAZIT: DER UMGANG MIT DEM RECHT AUF AUSKUNFT IST VERBESSERUNGSWÜRDIG

Das Recht auf Auskunft bildet somit eine weitere wichtige Säule im transparenten Umgang der elektronischen Bezahldienstleister mit Verbraucherdaten. Mit Anwendung der DSGVO wird dieses umfangreicher ausgestaltet sein. Die Ergebnisse der Untersuchung zeigen: Aktuell wird insbesondere die Verfahrensweise des Auskunftsprozesses von den Dienstleistern sehr unterschiedlich gehandhabt. Dies betrifft sowohl die Art der Reaktion als auch die Reaktionszeit. Während zwei Bezahldienstleister zunächst gar nicht auf die Auskunftsanfrage reagierten, beantworteten zwei Dienstleister die Anfrage mittels einer standardisierten Kunden-E-Mail, ohne Bezug auf das Anliegen zu nehmen. Ein Dienstleister hingegen veranlasste sofort das Auskunftsschreiben an die betreffende Person. PayPal und Skrill knüpften an die Erlangung der Auskunft ein Entgelt oder die Übersendung eines nicht im Sinne des Bundesbeauftragten für den Datenschutz und die Informationssicherheit geschwärzten Identitätsnachweises. SOFORT Überweisung kam der Bitte um Auskunft mittels geschwärzten Identitätsnachweises nach. Die Dauer zwischen der ersten Anfrage und der Übermittlung der Auskunftsschreiben variierte bei den untersuchten Dienstleistern zwischen zwei Tagen im Minimum und 62 Tagen im Maximum.

Die in den vorliegenden Auskünften übermittelten Inhalte entsprechen überwiegend den im Auskunftsschreiben erbetenen Informationen. Auch stimmen die Angaben zu den gespeicherten Daten mit den Angaben in den jeweiligen Datenschutzerklärungen der Bezahldienstleister überein. So machen paydirekt und SOFORT Überweisung in ihren Auskünften Angaben zu Art, Zweck, Herkunft und Übermittlung an Dritte von Daten und weisen darauf hin, dass sie weder Daten zur Erstellung von Nutzungsprofilen noch von Scorewerten erheben. Amazon Pay nimmt in seinem Auskunftsschreiben Bezug auf alle das Amazon-Nutzerkonto betreffende Daten. Angaben zur Erstellung von Nutzerprofilen oder Scorewerten werden nicht gemacht.

Die Auskunftsschreiben können, wie schon die Datenschutzerklärungen der Bezahldienstleister, als schwer verständlich gewertet werden. Als einzige positive Ausnahme ist hier das Auskunftsschreiben von paydirekt zu bewerten.

6. VERBRAUCHERERWARTUNG AN DEN DATENSCHUTZ

Neben dem Grundrecht auf informationelle Selbstbestimmung verlangt eine Datenerhebung und -verwendung über den vertraglichen Zweck der Dienstleistung hinaus in bestimmten Fällen eine explizite Einwilligung des Betroffenen. Voraussetzung zur Einwilligung ist dessen Informiertheit. Sowohl die Informiertheit als auch die Einwilligung werden in der gängigen Praxis über die Datenschutzerklärung gewährleistet bzw. eingeholt. Zu beachten ist hier jedoch, dass diese vorrangig der Informiertheit dienen soll[117] und in wenigen Passagen einwilligungsrelevante Tatbestände enthält. Wie in Kapitel 4 dargelegt, sind die Datenschutzerklärungen als unverständlich bis schwer verständlich zu bewerten und das Lesen sehr zeitaufwendig. So verwundert es auch nicht, dass mehr als drei Viertel der Internetnutzer angeben, den zur Verfügung gestellten Datenschutzerklärungen zuzustimmen, ohne sie wirklich verstanden zu haben[118]. Vor diesem Hintergrund werden nachfolgend Verbrauchermeinungen und -erwartungen aus repräsentativer Befragung[119] vorgestellt. Auf dieser Basis werden Aussagen dazu gemacht, welche Daten Verbraucher bereit wären, elektronischen Bezahldienstleistern zur Verfügung zu stellen, worüber und mit welchen Formaten sie informiert werden wollen und ob sie von ihrem Recht auf Auskunft Gebrauch machen möchten.

WELCHE DATEN WÜRDEN VERBRAUCHER WEITERGEBEN?

In der gängigen Praxis müssen Verbraucher vor Nutzung des Bezahldienstes der Datenschutzerklärung des jeweiligen Dienstleisters zustimmen. Damit soll erreicht werden, dass der Einzelne umfassend informiert ist und seinem Recht auf informationelle Selbstbestimmung Folge leisten kann. Dies betrifft auch die Informiertheit über die Erhebung, Speicherung und Verarbeitung seiner personenbezogenen Daten.

Auf die offene Frage, ob überhaupt und welche Daten Verbraucher bereit sind, bei Nutzung eines elektronischen Bezahldienstes an den Dienstleister weiterzugeben, haben 74 Prozent der Befragten konkrete Vorstellungen. Nahezu die Hälfte der Befragten (42 Prozent) gibt an, Stammdaten wie Name, Geburtsdatum und Kontaktdaten angeben zu wollen. 21 Prozent benennen ebenfalls die Bankverbindungsdaten. Nahezu jeder Fünfte (17 Prozent) äußert bei freier Entscheidung, nur die zur Abwicklung einer Zahlung wirklich notwendigen Daten bzw. so wenig Daten wie möglich weitergeben zu wollen. Diese Haltung verdeutlichen die in **Abbildung 12** (siehe Seite 38) ausgewählten Zitate der Befragten. Auch wird aus den Zitaten deutlich, dass sich die Befragten durchaus der Datenerhebung und -verwendung bewusst sind, ihr Wunsch jedoch dahin geht, wenig von sich preisgeben zu müssen.

Bei gestützter Nachfrage sind es vor allem Daten zur Kredithistorie (78 Prozent), dem eigenen Nutzungsverhalten beim Online-Händler (78 Prozent) sowie zum Standort während des Bezahlens (76 Prozent), die die Befragten nicht preisgeben möchten. Ebenso auf Ablehnung stößt die Preisgabe von vorgemerkten Waren beim Online-Händler (67 Prozent), der Kontodeckung (63 Prozent) sowie der IP-Adresse (66 Prozent) und des genutzten Gerätetyps (60 Prozent). Dahingegen würden die Befragten Daten wie Namen (78 Prozent), Zahlungsbetrag (73 Prozent), Händlernamen (65 Prozent), Uhrzeit (55 Prozent) und Bankverbindung (50 Prozent) überwiegend weitergeben (vgl. **Abbildung 13**, Seite 39).

117 Nach BDSG muss unter bestimmten Voraussetzungen in der Datenschutzerklärung auch über das Auskunftsrecht informiert werden. Ab Mai 2018 muss nach DSGVO generell über die Betroffenenrechte informiert werden.

118 Vgl. Rohleder (2015): Datenschutz in der digitalen Welt, Bitkom, online verfügbar unter: https://www.bitkom.org/Presse/Anhaenge-an-PIs/2015/09-September/Bitkom-Charts-PK-Datenschutz-22092015-final.pdf, Stand 07.08.2017.

119 Computergestütztes Webinterview (CAWI) unter n = 2.001 Nutzern elektronischer Bezahlverfahren ab 18 Jahren in Deutschland anhand eines strukturierten Fragebogens im Online-Panel forsa.omninet.

12 ZITATE ZUR WEITERGABE PERSÖNLICHER DATEN BEI FREIER ENTSCHEIDUNG

Basis: n = 2.001 Nutzer elektronischer Bezahldienste, offene Frage. **Frage:** Wenn Sie einen Bezahldienstleister nutzen, stimmen Sie in der Regel im Vorfeld der Verwendung ihrer persönlichen Daten zu. Wenn Sie nun frei entscheiden könnten, welche Ihrer Daten würden Sie an den Bezahldienstleister weitergeben?

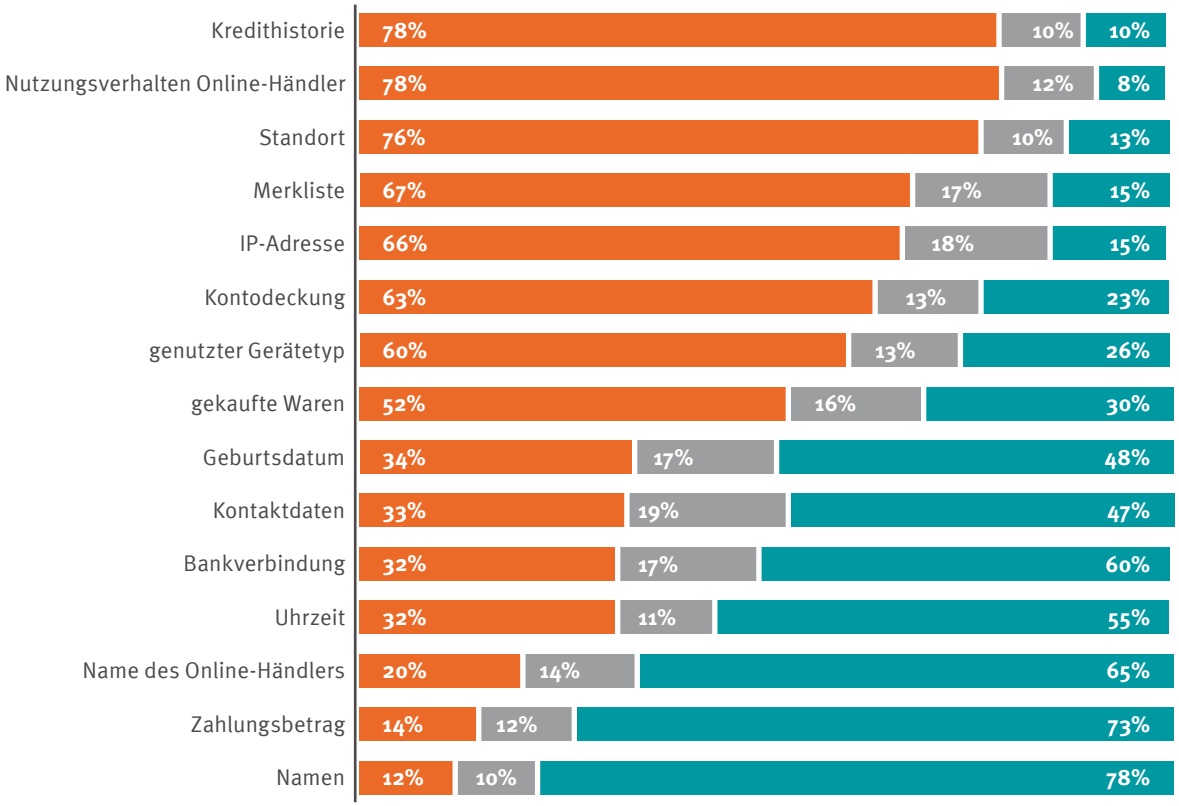
Frauen zeigen sich hinsichtlich der Weitergabe ihrer Daten zurückhaltender und insbesondere die Preisgabe der IP-Adresse stößt bei ihnen auf stärkere Ablehnung (72 Prozent) als bei Männern (60 Prozent). Auch zwischen den Altersgruppen zeigen sich Unterschiede in der Bereitschaft Daten weiterzugeben: Während beispielsweise Nutzer ab 50 Jahren weniger bereit sind als die unter 30-Jährigen ihre Kontodeckung preiszugeben (70 Prozent versus 48 Prozent), lehnen jüngere Nutzer stärker die Weitergabe von Standortdaten (82 Prozent versus 69 Prozent) und gekauften Waren (55 Prozent versus 45 Prozent) ab.

IN WELCHEM UMFANG WOLLEN VERBRAUCHER INFORMIERT WERDEN?

Die deutliche Mehrheit der befragten Nutzer elektronischer Bezahlverfahren (82 Prozent) möchte vollständig über den Umgang des Bezahldienstleisters mit ihren persönlichen Daten informiert werden (vgl. **Abbildung 14**, Seite 39). Zwei Drittel (64 Prozent) wollen dies möglichst in einem kurzen und knappen Format. Die Bereitschaft ausführliche Informationen zu lesen, um vollständig informiert zu sein, ist dagegen deutlich geringer: Nur jeder sechste Befragte (18 Prozent) ist hierzu bereit. 15 Prozent der Befragten geben an, ausschließlich für die Person relevante Informationen erhalten zu wollen. Ein Prozent der befragten Nutzer elektronischer Bezahldienstleister wünscht sich keinerlei Informationen zur Erhebung und Verwendung ihrer Daten durch den Dienstleister.

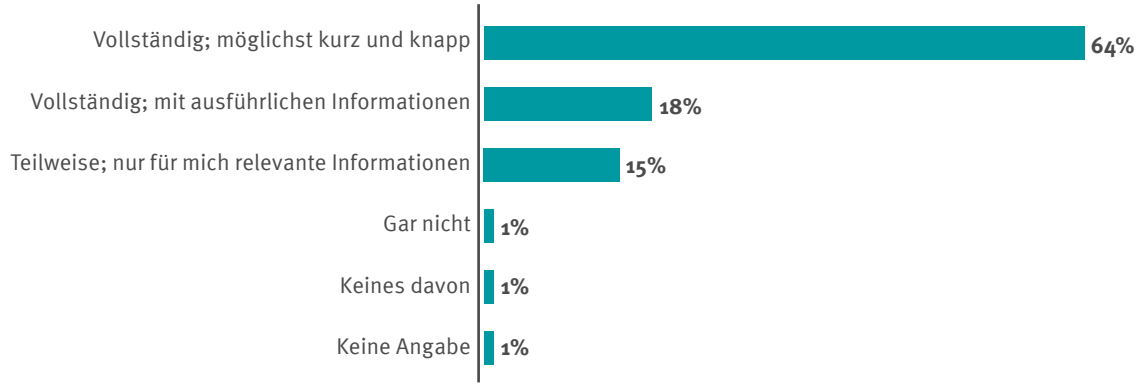
Auf die Frage, wie viel Zeit die Nutzer für das Lesen der Information zur Verwendung ihrer persönlichen Daten auf der Internetseite des Bezahldienstleisters maximal aufwenden wollen, spricht sich nahezu die Hälfte (46 Prozent) für einen Zeitaufwand zwischen drei bis fünf Minuten aus. Ein Drittel (31 Prozent) würde ein bis zwei Minuten investieren wollen. Ein Fünftel der Befragten (23 Prozent) ist bereit, mehr als fünf Minuten zu investieren. Die Bereitschaft ein Dokument zur Datenaufklärung länger als 10 Minuten zu lesen, äußert weniger als ein Zehntel der Befragten (8 Prozent). Die Bereitschaft mehr als 10 Minuten zu investieren, steigt

13 BEREITSCHAFT ZUR WEITERGABE VON DATEN AN BEZAHLDIENSTLEISTER



Legende: ■ = "Würde ich nicht weitergeben" ■ = "Bin mir nicht sicher" ■ = "Würde ich weitergeben"
Basis: n = 2.001 Nutzer elektronischer Bezahldienste; geschlossene Frage: **Frage:** Sie sehen nun einige persönliche Daten. Welche davon würden Sie an den Bezahldienstleister weitergeben und welche nicht?

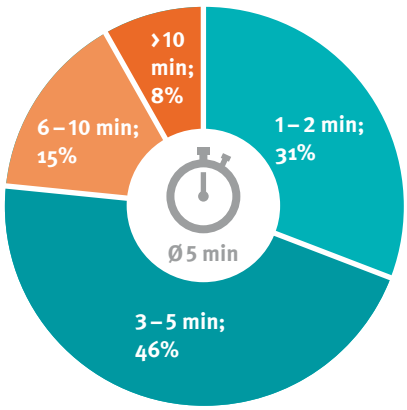
14 ANFORDERUNGEN DER NUTZER AN DEN UMFANG DER INFORMATIONEN



Basis: n = 2.001 Nutzer elektronischer Bezahldienste; geschlossene Frage. **Frage:** Wie umfangreich sollten die Informationen zur Erhebung und Verwendung ihrer persönlichen Daten auf der Internetseite des Bezahldienstleisters sein?

tendenziell etwas mit zunehmenden Alter (11 Prozent bei Nutzern ab 50 Jahren versus 6 Prozent bei Nutzern unter 30 Jahren). Somit wären rund 5 Minuten der Zeitaufwand, den die Befragten für das Lesen der Informationen zur Verwendung ihrer persönlichen Daten im Durchschnitt aufwenden würden. **Abbildung 15** stellt die Dauer der Lesebereitschaft dar.

15 PRÄFERIERTE ZEIT DER NUTZER ZUM LESEN DER INFORMATIONEN



Basis: n = 1.768 Nutzer elektronischer Bezahldienste, die Angaben zur Lesedauer gemacht haben; offene Frage.
Frage: Wie viel Zeit würden Sie für das Lesen der Information zur Verwendung ihrer persönlichen Daten auf der Internetseite des Bezahldienstleisters maximal aufwenden wollen? Bitte nennen sie eine konkrete Zeit in einer Zeiteinheit (z.B. Minuten).

IN WELCHER FORM WOLLEN VERBRAUCHER INFORMIERT WERDEN?

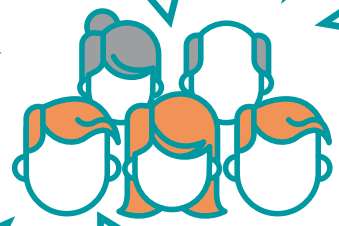
Offen befragt formuliert die Hälfte (48 Prozent) der Nutzer elektronischer Bezahldienstleister Ideen über geeignete Gestaltungsformate zur Information über die Datenpraxis der Bezahldienstleister. Unter den Vorstellungen finden sich allen voran Formate, die eine zusammenfassende (19 Prozent), übersichtliche (17 Prozent), verständliche (11 Prozent) und transparente (10 Prozent) Darstellung der Informationen erlauben. Datenschutzerklärungen im heutigen Format benennen nur wenige der Befragten (7 Prozent) mit konkreten Vorstellungen.

Abbildung 16 stellt ausgewählte Zitate der Befragten dar. Die Zitate verdeutlichen zudem den Wunsch nach einer Form von Checkliste, die darüber informiert, welche Daten zu welchen Zweck erhoben werden, verbunden mit der aktiven Wahl des Verbrauchers, welche der Daten man tatsächlich preisgeben möchte.

Gibt man Gestaltungsformate zur Auswahl vor, bewertet über die Hälfte der Befragten ein einseitiges Schriftstück mit konkreter Auflistung, welche Daten zu welchem Zweck verwendet werden, als gut geeignet (60 Prozent) **(vgl. Abbildung 17)**. Nahezu jeder Zweite (45 Prozent) hält ein Siegel einer unabhängigen Institution, das nur darüber informiert, ob der Dienst seriös ist, für gut geeignet. Ein interaktives Dokument mit zunächst kurzer, dann detaillierter Auflistung können sich 40 Prozent der Befragten gut vorstellen. Ein einseitiges Schriftstück mit bildlicher Darstellung wird von jedem dritten Befragten (33 Prozent) als gut geeignet befunden. Jeder Zehnte (11 Prozent) findet einen animierten Kurzfilm geeignet, ihn zu informieren. Ebenso jeder Zehnte (10 Prozent) bewertet das heute übliche mehrseitige Schriftstück mit detaillierten Informationen als gut geeignetes Format.

Bei der Bewertung des geeignetsten Formates favorisieren die Befragten (36 Prozent) das einseitige Schriftstück mit konkreter Auflistung, welche Daten zu welchem Zweck verwendet werden. Beim präferierten Format gibt es jedoch leichte Altersunterschiede: Während Nutzer ab 50 Jahren deutlich das Format des einseitigen Schriftstücks mit konkreter Auflistung (43 Prozent) präferieren, sprechen sich jüngere Befragte bis 30 Jahre neben einem einseitigen Schriftstück (24 Prozent) am häufigsten für ein interaktives Dokument (25 Prozent) aus. Unabhängig von Alter und Geschlecht hält nahezu keiner der Befragten (4 Prozent) ein mehrseitiges Informationsdokument – und damit die gängige Praxis – für am besten geeignet.

16 ZITATE ZU FORMATEN ZU INFORMATIONEN DER DATENPRAXIS



"Nach Grundsätzen der Datensparsamkeit sind eigentlich nur Daten zu erheben, die zur Vertragsabwicklung notwendig sind, daher würde ich mir eine Aufklärung darüber wünschen, warum gerade die erhobenen Daten notwendig sind. Darüber hinaus, wie lange sie gespeichert werden. UND ob sie mit bereits vorhandenen Daten aus anderen Transaktionen verknüpft werden, und wenn ja, warum."

"Vollständige, LEICHT VERSTÄNDLICHE Auflistung der möglichen Datenmengen; absolut notwendige nicht abwählbar, alle anderen mit entfernbaren Häkchen."

"Übersicht der Daten, die weiterverarbeitet werden und direkt eine Option zum Widerruf möglicher freigebener Daten."

"Es sollte vor jeder Zahlung, bevor ich auf die Seite der Zahlungsabwicklungsfirma geleitet werde, ein Fenster angezeigt werden, wo steht, was weitergegeben wird, so dass ich mir ggf. eine andere Zahlungsart aussuchen kann."

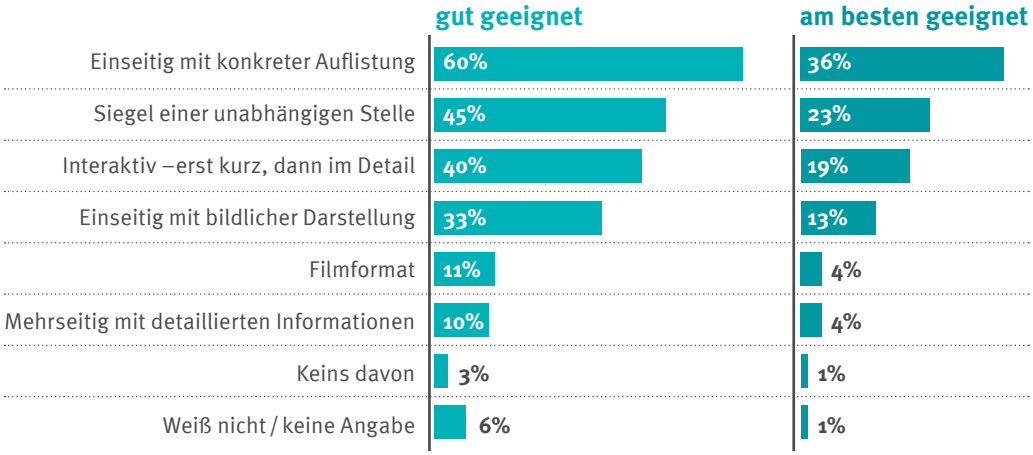
"So, dass ich selbst frei entscheiden kann, welche Daten gespeichert und weitergegeben werden, also eine eigene Matrix zur Entscheidung, welche Daten ich preisgeben möchte und welche nicht."

"Jeder Punkt, der erhoben wird, sollte einzeln zu- oder abgewählt werden können. Eine Gesamtzustimmung sollte es nicht geben."

"Konkrete Auflistung, welche Daten für welchen Zweck verwendet werden, es bringt mir nichts nur zu wissen welche Daten, ich möchte auch wissen, wofür sie verwendet werden."

Basis: n = 2.001 Nutzer elektronischer Bezahldienste, offene Frage. **Frage:** Bisher werden Sie meist in Form einer Datenschutzerklärung darüber informiert, welche Ihrer persönlichen Daten erhoben und verarbeitet werden. Wenn Sie frei entscheiden könnten: In welcher Form würden Sie sich die Information zur Verwendung Ihrer persönlichen Daten auf der Internetseite eines Bezahldienstleisters wünschen?

17 EIGNUNG VERSCHIEDENER INFORMATIONSFORMATE AUS SICHT DER VERBRAUCHER



Basis: n = 2.001 Nutzer elektronischer Bezahldienste bzw. n = 1.840 Nutzer elektronischer Bezahldienste, die mindestens ein Format als geeignet bewertet haben; geschlossene Frage. **Fragen:** Welche der nachfolgenden Gestaltungsformate finden Sie gut geeignet, um Sie über die Erhebung und Verwendung Ihrer persönlichen Daten auf der Internetseite eines Bezahldienstleisters zu informieren? (Mehrfachnennung möglich). Und wenn Sie sich für ein Gestaltungsformat zur Information über die Erhebung und Verwendung Ihrer persönlichen Daten auf der Internetseite eines Bezahldienstleisters entscheiden müssten: Welches Format finden Sie am besten geeignet?

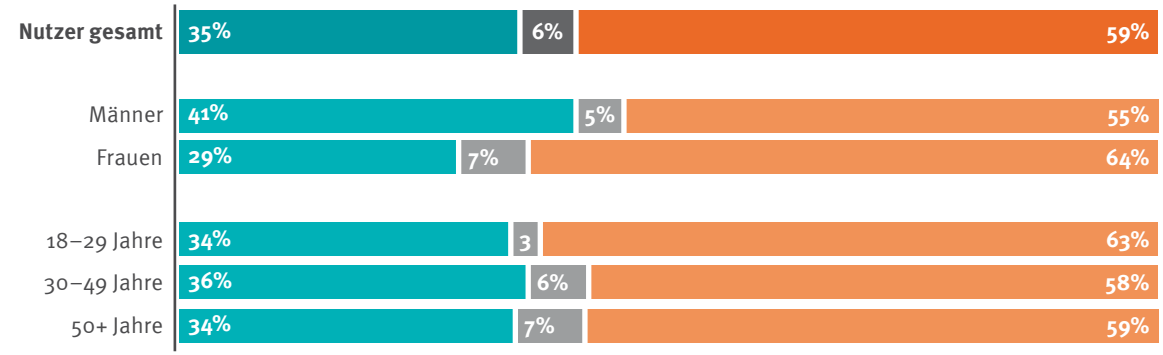
KENNEN UND WÜNSCHEN VERBRAUCHER DAS RECHT AUF AUSKUNFT?

Kenntnis darüber, ob und welche persönlichen Daten zur eigenen Person erhoben und gespeichert werden, können Verbraucher nicht nur mittels der in der Datenschutzerklärung bereitgestellten Informationen der Bezahldienstleister erlangen: Nach Nutzung der Dienstleistung besteht darüber hinaus das Recht auf Auskunft des Betroffenen (vgl. Kapitel 5).

Wie sich zeigt, kennt aktuell nur ein Drittel der Nutzer elektronischer Bezahlverfahren (35 Prozent) das Auskunftsrecht. Deutlich mehr als die Hälfte der Befragten (59 Prozent) gibt an, nicht zu wissen, dass sie von ihrem Recht aus Auskunft Gebrauch machen können. **Abbildung 18** stellt dar, wie viele der Befragten heute von ihrem Recht auf Auskunft wissen.

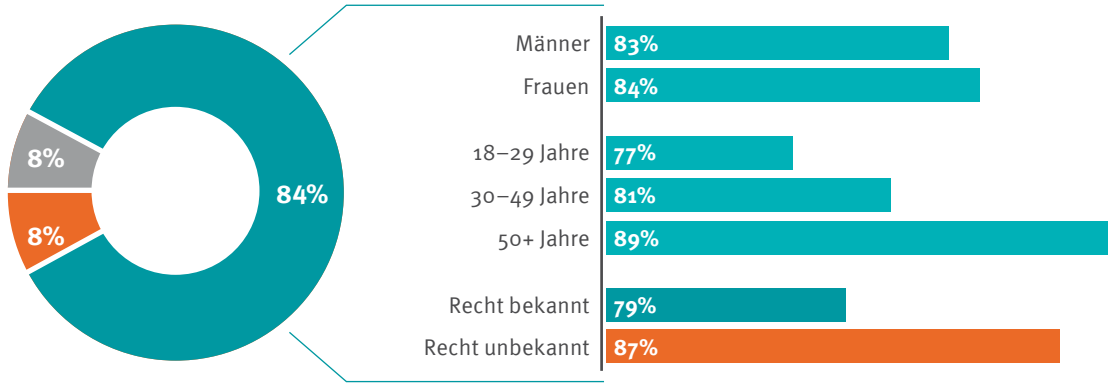
Im Gegensatz dazu besteht bei einer deutlichen Mehrheit der befragten Nutzer (84 Prozent) der Wunsch, konkrete Informationen vom Bezahldienstleister zur Erhebung und Verwendung personenbezogener Daten zu erhalten **(vgl. Abbildung 19)**. Weniger als jeder Zehnte verneint hier bzw. gibt an, nicht zu wissen, ob er diese Informationen möchte (jeweils 8 Prozent). Vor allem Nutzer ab 50 Jahren geben dagegen an, Auskunft über die Erhebung und Verwendung ihrer persönlichen Daten haben zu wollen (89 Prozent). Zudem zeigt sich, dass der Wunsch Auskunft zu erhalten insbesondere bei denjenigen Befragten besteht, die bisher nichts von ihrem Auskunftsrecht wussten (87 Prozent).

18 KENNTNIS DES GESETZLICHEN RECHTS AUF AUSKUNFT NACH § 34 BDSG



Legende: ■ = Ja ■ = Weiß nicht ■ = Nein
Basis: n = 2.001 Nutzer elektronischer Bezahldienste; Männer n = 1.026, Frauen n = 975, 18- 29 Jährige n = 358, 30- 49 Jährige n = 749, 50+ Jährige n = 895; geschlossene Frage. **Frage:** Allerdings haben Sie ein gesetzliches Recht darauf, auf Wunsch eine Auskunft zur Erhebung und Verwendung ihrer persönlichen Daten durch den Bezahldienstleister zu erhalten. War Ihnen das bekannt?

19 WUNSCH, AUSKUNFT VOM BEZAHLDIENSTLEISTER ZU ERHALTEN



Legende: ■ = Ja ■ = Weiß nicht ■ = Nein
Basis: n = 2.001 Nutzer elektronischer Bezahldienste; Männer n = 1.026, Frauen n = 975, 18- 29 Jährige n = 358, 30- 49 Jährige n = 749, 50+ Jährige n = 895, Recht bekannt n = 698, Recht unbekannt n = 1.187; geschlossene Frage. **Frage:** Würden Sie gerne über die konkrete Erhebung und Verwendung Ihrer persönlichen Daten durch die von Ihnen genutzten Bezahldienstleister Auskunft erhalten?

FAZIT: AUFTRAG DER VERBRAUCHER – KURZE, VERSTÄNDLICHE DATENSCHUTZ-ERKLÄRUNGEN MIT ENTSCHEIDUNGS-MÖGLICHKEIT

Vor dem Hintergrund der gängigen Praxis wurden Verbraucher in offenen und geschlossenen Fragen um ihre Erwartungen hinsichtlich des transparenten Umganges mit ihren personenbezogenen Daten gebeten. Im Ergebnis zeigt sich, dass Nutzer elektronischer Bezahlverfahren in der Mehrheit konkrete Vorstellungen haben, welche Daten sie ohne Bedenken zur Nutzung des Dienstes preisgeben würden. Hierzu gehören Daten wie Name, Geburtsdatum, Kontaktdaten sowie die Bankverbindungsdaten. Es zeigt sich aber auch, dass nahezu jeder Fünfte (17 Prozent) von sich aus klar formuliert, dass es ihm wichtig ist, nur die wirklich notwendigen Daten von sich offen zu legen. Insofern wird das Prinzip der Datensparsamkeit verbraucherseitig deutlich gefordert. Daten, die mehr als drei Viertel der Befragten nicht weitergeben wollen, sind: Daten zur eigenen Kredithistorie (78 Prozent), dem Nutzungsverhalten (78 Prozent) und dem Standort (76 Prozent).

Eine klare Mehrheit der Befragten (64 Prozent) spricht sich für ein kurzes Format mit vollständiger Information aus. Hierfür sind die Befragten bereit, einen Zeitaufwand von durchschnittlich fünf Minuten für das Lesen der Informationen aufzuwenden. Aktuell benötigt ein Leser beispielsweise für das Lesen der Datenschutzerklärung von PayPal 24 Minuten (siehe Kapitel 4) – dies übersteigt die Bereitschaft deutlich.

Frei befragt nach der Gestaltung der Informationen zur Datenpraxis, benennen die Befragten insbesondere eine zusammenfassende, übersichtliche, verständliche und transparente Darstellung. Daneben sind es Formate im Sinne einer Checkliste, bei denen Nutzern transparent dargestellt wird, welche Daten zu welchen Zwecken verwendet werden, verbunden mit einer aktiven Wahl bzw. Abwahl von Einzeldaten. Gestützt als das Format der Wahl und damit als am besten geeignet, bewerten die Befragten (36 Prozent) ein einseitiges Schriftstück mit konkreter Auflistung der Einzeldaten verbunden mit dem Zweck der Verwendung. Mehrseitige Schriftstücke – wie aktuell die gängige Praxis – werden nur von sehr wenigen Befragten (4 Prozent) präferiert.

Vom Recht auf Auskunft weiß nur ein Drittel (35 Prozent) der Befragten. Im Gegensatz dazu, besteht bei der deutlichen Mehrheit der befragten Nutzer (84 Prozent) der Wunsch, Auskunft vom genutzten Bezahldienstleister zu erhalten. Insofern besteht bei den Verbrauchern dringender Bedarf nach adäquater Aufklärung über ihre Rechte.

7. SCHLUSSFOLGERUNGEN

Einkaufen im Internet ist bei den Verbrauchern in Deutschland angekommen: 2016 nutzten nahezu 50 Millionen das Internet[120]. Laut dem deutschen Institut für Vertrauen und Sicherheit im Internet kaufen von den Internetnutzern nahezu 98 Prozent zumindest gelegentlich online ein[121]. Die Bezahlung via elektronische Bezahlverfahren ist ebenfalls weit verbreitet: Über 30 Millionen Nutzer in Deutschland[122] machen davon Gebrauch. Nicht jedem ist dabei wohl: Als wesentliche Hemmnisse benennen Verbraucher Datensicherheit und die Verwendung ihrer Daten durch die elektronischen Bezahldienstleister.

DATENSICHERHEIT: BEZAHLDIENSTLEISTER SICHERN WEITGEHEND HOHES NIVEAU FÜR IHRE KUNDEN

Die untersuchten elektronischen Bezahldienstleister kommen ihrer Verantwortung nach Datensicherheit für ihre Nutzer zum Teil nach. Das Sicherheitsniveau ist, gemessen an allgemeinen Web-Anwendungen, vergleichsweise hoch. Die Verschlüsselung der Kommunikation zwischen dem Browser des Nutzers und dem Server des elektronischen Bezahldienstleisters wird vom externen Gutachter als sicher eingeschätzt. Daneben wird eine sichere Anmeldung durch eine 2-Faktor-Authentifizierung über SMS-TAN gewährleistet. Die Benutzersitzung ist ebenfalls gut absichert. Gegen Phishing-Angriffe gibt es durchgängig keinen wirksamen Schutz. Einen zusätzlichen Schutz über eine Content Security Policy implementieren nicht alle Dienstleister: So verzichten giropay, SOFORT Überweisung und Skrill bis dato darauf.

DATENSPARSAMKEIT: NICHT JEDER BEZAHLDIENSTLEISTER FOLGT IHR GLEICHERMASSEN

Hinsichtlich der Einhaltung des Prinzips der Datensparsamkeit verfolgen die Bezahldienstleister unterschiedliche Ansätze. So variiert die Anzahl erhobener Nutzer-Daten durch die Bezahldienstleister bei Registrierung und Bezahlvorgang zwischen vier und 13 Einzeldaten. Dienste ohne Registrierung wie giropay und SOFORT Überweisung erheben vergleichsweise wenige Daten. Auch die Anzahl übermittelter Daten zwischen Händler und Bezahldienstleister unterscheidet sich: Paydirekt und PayPal tauschen deutlich mehr Daten mit dem Händler aus. Amazon Pay hat zudem Zugriff auf das Amazon-Nutzerkonto.

Tracking-Dienste zur Erhebung von Nutzerdaten setzen die elektronischen Bezahldienstleister in unterschiedlichem Maß ein: Während paydirekt auf die Nutzung eines externen Dienstes setzt, binden Amazon Pay und giropay jeweils zwei und SOFORT Überweisung vier Tracking-Dienste ein. Deutlich mehr Dienste verwenden PayPal mit sieben und Skrill mit elf auf ihren öffentlich zugänglichen Web-Auftritt. Zwei Bezahldienstleister binden auch im privaten Bereich Tracking ein: Paydirekt den Dienst Webtrekk, der jedoch nach eigenen Angaben keine personenbeziehbaren Daten erhebt und die Nutzer-Daten nicht mit Dritten teilt. Skrill verwendet vier Tracking-Dienste, die alle nach eigenen Angaben auch personenbeziehbare Daten erheben. Zwei von ihnen geben diese personenbeziehbaren Daten auch an Dritte weiter.

DATENSCHUTZERKLÄRUNGEN: LASSEN INTERPRETATIONSSPIELRAUM UND SIND SCHWER VERSTÄNDLICH

Skrill stellt keine dienstleistungsbezogene Datenschutzerklärung zur Verfügung. Alle weiteren untersuchten Bezahldienstleister informieren in den Datenschutzerklärungen im Rahmen der gesetzlichen Anforderungen. Konkrete Aussagen finden sich in allen Erklärungen dazu, dass personenbezogene Daten erhoben und Daten an Dritte weitergeben werden. Angaben zur Art der erhobenen personenbezogenen Daten, der Art der

120 Hochrechnung der Befragungsergebnisse 2016, n=2.012, Basis Hochrechnungen: Statistisches Bundesamt und forsa-Mehrthemenbus, Dautzenberg et al. (2017b): Nutzung elektronischer Bezahlsysteme: Werden Datenschutzbestimmungen vom Verbraucher gelesen?, online verfügbar unter: https://ssl.marktwaechter.de/sites/default/files/downloads/infografik-datenschutz-elektronische-bezahlsysteme.pdf, Stand 07.08.2017.

121 Vgl. Deutsches Institut für Vertrauen und Sicherheit (2015): Einkaufen in der digitalen Welt, online verfügbar unter: https://www.divsi.de/wp-content/uploads/2015/08/2015-08-18-Online-Shopping_web.pdf, Stand 07.09.2017, S. 6.

122 Vgl. Dautzenberg et al. (2017b).

weitergegebenen Daten und den jeweiligen Empfängern der Daten werden nicht von jedem Bezahldienstleister abschließend gegeben. Hier tragen Wortwendungen wie „zum Beispiel“, „möglicherweise“ und „unter anderem“ zu erheblichen Interpretationsspielraum bei. Verbraucher können anhand dieser Formulierungen nicht erkennen, worauf sie sich bei Nutzung des Dienstes konkret einlassen.

Amazon Pay und PayPal nutzen die erhobenen Daten neben der Erfüllung der Vertrags- und Sicherheitszwecke auch für Marketingzwecke sowie die Bereitstellung personalisierter Angebote. Einen aktiven Einfluss, zu welchen Zwecken seine Daten verwendet werden, kann der Nutzer nicht nehmen.

Die formale Verständlichkeit der untersuchten Datenschutzerklärungen bewegt sich zwischen unverständlich und schwer verständlich. So sind es insbesondere lange Sätze, Passivkonstruktionen und Füllwörter, die dem Leser die Verständlichkeit erschweren. Die Länge der Erklärungen und damit der zeitliche Aufwand für die Nutzer variiert stark: Das Lesen der Datenschutzerklärung von SOFORT Überweisung verlangt dem Leser vier Minuten Lesezeit ab. Zum Lesen der Datenschutzerklärung von paydirekt müssen gut sechs Minuten und von Amazon Pay 15 Minuten aufgewendet werden. Im Fall von PayPal benötigt ein Nutzer sogar 24 Minuten Lesezeit. Berücksichtigt man die 48-seitige Liste[123], in der aufgeführt wird, welche Daten an welche Dritte weitergegeben werden, steigt der Aufwand für die Nutzer nochmals erheblich.

RECHT AUF AUSKUNFT: DIE VERFAHRENSWEISE IST VERBESSERUNGSWÜRDIG

Die Verfahrensweise der Bezahldienstleister beim Auskunftsprozess ist sehr heterogen: Die Reaktionen auf das erste Auskunftsersuchen reichen von sofortiger Auskunft (paydirekt, SOFORT Überweisung), über standardisierte Kunden-E-Mails ohne Bezug zum Anliegen (Amazon Pay, PayPal) bis zu gar keiner Reaktion (giropay, Skrill). Skrill knüpft an die Erlangung der Auskunft ein Entgelt und Paypal verlangt die Übersendung eines Identitätsnachweises mit sichtbarer Identifikationsnummer des Personalausweises. SOFORT Überweisung kommt der Bitte auf Auskunft nach Zusenden eines geschwärzten Identitätsnachweises in nur zwei Tagen nach. Die Verfahrensdauer zwischen erstem Auskunftsersuchen und Übermittlung der Auskunftsschreiben variiert zwischen zwei und 62 Tagen.

Die in den vorliegenden Auskünften übermittelten Inhalte entsprechen überwiegend den im Auskunftsersuchen erbetenen Informationen. Die Angaben zu den gespeicherten Daten stimmen mit den Angaben in den jeweiligen Datenschutzerklärungen der Bezahldienstleister überein. Die Auskunftsschreiben sind formal schwer verständlich. Positive Ausnahme ist hier das Auskunftsschreiben von paydirekt.

VERBRAUCHERMEINUNG: GEFORDERT WERDEN PRÄGNANTE, VERSTÄNDLICHE INFORMATIONEN MIT ENTSCHEIDUNGSFREIHEIT

Nutzer elektronischer Bezahlverfahren benennen offen konkrete Vorstellungen, welche Daten sie zur Nutzung des Dienstes preisgeben würden: Name, Geburtsdatum, Kontaktdaten und Bankverbindungsdaten. Nahezu jeder Fünfte äußert bei freier Entscheidung, nur die zur Abwicklung einer Zahlung wirklich notwendigen Daten bzw. so wenig Daten wie möglich weitergeben zu wollen. Dies verdeutlicht nachfolgende Verbrauchermeinung: „Grundsätzlich nur die Daten, welche tatsächlich nötig sind, um auf mein Konto einmaligen Zugriff zu haben. Dazu gehört schätze ich Name, Kreditinstitut, IBAN/ BIC und die einmalige Zugrifferlaubnis…“. Daten zur eigenen Kredithistorie, dem Nutzungsverhalten und dem Standort möchten die befragten Nutzer bei gestützter Nachfrage überwiegend nicht von sich preisgeben.

Auch zum Informationsformat herrscht Klarheit bei den Nutzern: Dieses sollte kurz, übersichtlich, verständlich und transparent darlegen, welche Daten erhoben, verarbeitet und weitergeben werden. Für das Lesen einer Datenschutzerklärung sind die Befragten im Durchschnitt bereit, fünf Minuten Lesezeit zu investieren. Als am besten geeignet bewerten die Befragten (36 Prozent) ein einseitiges Schriftstück. Dieses sollte eine konkrete Auflistung der Einzeldaten enthalten, verbunden mit dem Zweck der Verwendung. Ein mehrseitiges

123 Vgl. PayPal (2017b): PayPal-Datenschutzgrundsätze, online verfügbar unter: https://www.paypal.com/de/webapps/mpp/ua/privacy-full?locale.x=de_DE, Stand 01.07.2017.

Schriftstück – und damit die gängige Praxis – wird von nur sehr wenigen Befragten (4 Prozent) präferiert. Offen gefragt, wird der Wunsch nach einem Format deutlich, das eine aktive Wahl bzw. Abwahl von zu erhebenden Einzeldaten ermöglicht: „Jeder Punkt, der erhoben wird, sollte einzeln zu- oder abgewählt werden können. Eine Gesamtzustimmung sollte es nicht geben.“.

Ihr Recht auf Auskunft kennt gut ein Drittel der Befragten (35 Prozent). Im Gegensatz dazu besteht bei der deutlichen Mehrheit der befragten Nutzer (84 Prozent) der Wunsch, vom genutzten elektronischen Bezahldienstleister eine Auskunft über die Erhebung und Verwendung persönlicher Daten zu erhalten.

DISKREPANZ: VERBRAUCHERMEINUNG UND REALITÄT AM MARKT BEDÜRFEN DER ANNÄHERUNG

Dem geäußerten Wunsch (17 Prozent), nur die für die Bezahlung notwendigen Daten preiszugeben, kommen viele der untersuchen Dienstleister nicht nach: Sowohl bei Registrierung, Bezahlung, im Austausch mit dem Händler als auch durch Einbindung externer Tracking-Dienste werden umfangreich Nutzerdaten erhoben. Welche Daten genau erhoben werden, kann der Nutzer aus dem Lesen der Datenschutzerklärung vielfach nicht abschließend erfahren. Auch welche Daten weitergegeben werden und an wen, wird nicht immer ersichtlich. Amazon Pay und PayPal nutzen gemäß ihrer Datenschutzerklärung die erhobenen Daten für Marketingzwecke sowie zur Bereitstellung personalisierter Angebote. Auch dem Wunsch, bestimmte Einzeldaten nicht angeben zu müssen, kommen die Dienstleister nicht nach.

Dem Auftrag nach einem übersichtlichen, informativen einseitigen Format zur Information über erhobene und verarbeitete Daten wird derzeit nicht Rechnung getragen: Die Datenschutzerklärung von PayPal umfasst stattdessen sieben Seiten in der Schriftgröße Arial 5,5. Der Leseaufwand übersteigt deutlich die von den befragten Nutzern gewünschten fünf Minuten. Ein stärkerer Fokus auf relevante Inhalte, wie beispielsweise einwilligungsrelevante Tatbestände könnte helfen, die Prägnanz zu erhöhen und kurze Datenschutzerklärungen zu ermöglichen.

8. GLOSSAR

Bei der **2-Faktor-Authentifizierung** werden zwei Arten des Nachweises der Authentizität eines Benutzers kombiniert. Sie geht über die Standard-Anmeldung mit einem Passwort hinaus. Ein Beispiel für die 2-Faktor-Authentifizierung ist die Anmeldung mit Passwort und Transaktionsnummer[124].

Eine **Benutzersitzung (Session)** bezeichnet die Zeit zwischen dem Einloggen und dem Ausloggen des Benutzers. In dieser Zeit ist ein Zugriff auf die Benutzerdaten ohne Eingabe des Passworts möglich. Das üblichste Verfahren implementiert die Benutzer-Session über Cookies (s.u.), die die Zuordnung zum Nutzer (sog. Session-ID) speichern und automatisch mit jeder Anfrage an den Dienstleister übertragen. Bis das Cookie gelöscht wird, bleibt der Nutzer durch die Session-ID erkannt. Erlangt ein Angreifer die Session-ID, kann er alle Möglichkeiten nutzen, die dem Nutzer zur Verfügung stehen[125].

Eine **Bibliothek (Library)** ist ein zusätzlicher Programmbaustein, der häufig verwendete Systemroutinen enthält. Durch die Anbindung einer Bibliothek können Funktionen einfach abgerufen werden und müssen nicht neu implementiert werden[126].

Ein **Browser** ist eine Anwendung, die dem Nutzer Internetseiten anzeigt[127].

Mit einer **Browser-Erweiterung** können Nutzer ihren Browser (s.o.) um zusätzliche Funktionen ergänzen. Die Erweiterungen sind optional, d.h. der Browser kann auch ohne sie genutzt werden[128].

Durch **Chiffrierung** oder auch Verschlüsselung soll die Sicherheit bzw. Vertraulichkeit von Kommunikation gewährleistet werden. Hierfür gibt es verschiedene kryptografische Verfahren wie beispielsweise Strom- oder Blockchiffren oder den Austausch von Schlüsseln[129]. Für die Kommunikation im Internet stehen Verschlüsselungsprotokolle wie SSL (Secure Sockets Layer) oder TLS (s.u.) zur Verfügung[130]. In den letzten Jahren sind einige Angriffe auf bis dato häufig eingesetzte Protokollversionen bekannt geworden (z.B. BEAST, CRIME oder POODLE). Sie nutzen unterschiedliche Schwächen aus und betreffen üblicherweise einzelne Konfigurationen[131]. Nach Bekanntwerden einer Schwäche sollte die entsprechende Protokollversion nicht mehr eingesetzt werden[132]. Viele Server (s.u.) unterstützen jedoch veraltete oder unsichere Verschlüsselungsverfahren, damit auch ältere Browser (s.o.) auf die Webseite zugreifen können[133].

Ein **Client**, zum Beispiel ein Browser (s.o.), ist die Schnittstelle zwischen Nutzer und Netzwerk und oft für die Anzeige der Daten zuständig. Zur Darstellung der Daten richtet er eine Anfrage (Request) an den Server (s.u.) und erhält eine Antwort (Response)[134].

Mit einer **Content Security Policy (CSP)** sollen Webseiten vor Angriffen durch das Einschleusen von Daten durch Dritte geschützt werden (vgl. Cross-site Scripting (s.u.)). Hierfür wird definiert, aus welchen Quellen der Inhalt für eine Webseite kommen darf[135].

124 Vgl. BSI (2013): M 4.133 Geeignete Auswahl von Authentikationsmechanismen, online verfügbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04133.html, Stand 08.08.2017.

125 Vgl. BSI (2007): Web 2.0, Sicherheitsaspekte neuer Anwendungen und Nutzungsformen des Mediums World Wide Web und ihrer Implementierung, online verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Web20/web20_pdf.pdf?__blob=publicationFile&v=2, Stand 08.08.2017, S.23.

126 Vgl. Hofer/Fischer (2010): Lexikon der Informatik, 15. Auflage, Springer, S. 110.

127 Vgl. ebenda, S. 130.

128 Vgl. ebenda, S. 23.

129 Vgl. ebenda, S. 504-505.

130 Vgl. BSI (2015b): Die Lage der IT-Sicherheit in Deutschland, online verfügbar unter: https://www.bsi-fuer-buerger.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2015.pdf?__blob=publicationFile&v=5, Stand 08.08.2017, S. 7, 51.

131 Vgl. BSI (2015a): Empfehlung IT im Unternehmen, TLS/SSL Best Practice, online verfügbar unter: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_012.pdf;jsessionid=8F96D96295E8D67EF48F0074A01E8E51.1_cid369?__blob=publicationFile&v=4, Stand 08.08.2017, S. 1-2.

132 Vgl. ebenda, S. 6.

133 Vgl. BSI (2015b), S. 7.

134 Vgl. Hofer/Fischer (2010), S. 169.

135 Vgl. Kailas/Braun (2016): A Measurement Study of the Content Security Policy on Real-World Applications, International Journal of Network Security, Jg. 18, Nr.2, online verfügbar unter: https://www.researchgate.net/publication/285218986_A_easurement_study_of_the_content_security_policy_on_real-world_applications, Stand 08.08.2017, S. 383.

Cookies sind kleine Textdateien, die beim Besuch von Webseiten erstellt werden können und im Browser (s.o.) gespeichert werden. Sie enthalten beispielsweise Informationen über besuchte Webseiten oder Passwörter. Im Idealfall sollten Cookies verschlüsselt gesendet und temporär gespeichert werden[136].

Cross-site Scripting (XSS) ist ein Angriff, bei dem sich der Angreifer Kennungen wie Login-Name oder Passwort beschaffen will. Hierzu überwacht er die Interaktionen des Nutzers mit der Webseite und manipuliert Teile der Seite zu seinen Gunsten[137].

Ein **Extended Validation-Zertifikat** wird durch spezielle Zertifizierungsstellen vergeben. Es soll eine sichere Kommunikation verdeutlichen. Das Zertifikat wird durch den Browser (s.o.) überprüft. Ist es vertrauenswürdig, färbt sich die Adressleiste des Browsers grün[138].

Das **Frontend** einer Web-Anwendung ist der Teil, der auf Nutzerseite ausgeführt wird[139].

Ein **Host** ist ein Computersystem mit koordinierenden, steuernden Aufgaben in einem Verbund mehrerer Computersysteme[140].

HTTP (Hypertext Transfer Protocol) ist ein Protokoll zur Übertragung von Daten zwischen Client (s.o.) und Server (s.u.). Es wird beispielsweise dazu genutzt, Webseiten im Browser (s.o.) anzuzeigen[141].

Der **HTTP-Header** ist der Kopfbereich bei der Datenübertragung zwischen Client (s.o.) und Server (s.u.) im HTTP (s.o.). Ein Header übermittelt zusätzliche Informationen an das Gegenüber[142].

HTTPS (HTTPSecure) ist wie HTTP (s.o.) ein Übertragungsprotokoll. Durch Verschlüsselung (s.u.) stellt es eine sicherere Datenübertragung sicher[143].

Die **HSTS (HTTP Strict Transport Security**) ist eine Maßnahme, mit deren Hilfe eine Webseite dem Browser (s.o.) mitteilen kann, dass dieser die entsprechende Seite nur verschlüsselt (mit HTTPS (s.o.)) aufrufen darf. Dadurch sollen u.a. Man-in-the-Middle-Angriffe (s.u.) unterbunden werden[144].

Eine **IP-Adresse (Internet Protocol Address)** ist eine aus Zahlen bestehende Kennung, die jedem mit dem Internet verbundenen Gerät zugewiesen wird. Oftmals werden IP-Adressen benutzt, um Personen oder Unternehmen zu identifizieren, die über einen Internet-Anbieter ein Gerät mit dem Internet verbunden haben[145].

JavaScript ist eine Programmiersprache des Frontend (s.o.). Sie dient der Einbettung kleiner, häufig animierter oder interaktiver Objekte. JavaScript ermöglicht es, Funktionen im Browser (s.o.) direkt auszuführen[146].

Mit einer **Kryptoanalyse** sollen bestehende Verschlüsselungen (s.o.: Chiffrierung) entschlüsselt werden[147].

Der **Man-in-the-Middle** ist ein Lauscher auf dem Kommunikationskanal. Der Angreifer steht zwischen Sender und Empfänger und gibt sich als der jeweils andere aus. Er kann die ausgetauschten Daten sowohl mitlesen als auch bei Bedarf verändern[148].

Mit einem **Phishing-Angriff** versuchen Angreifer, an die Login-Daten eines Nutzers zu gelangen. Hierzu verwenden sie entweder eine gefälschte Webseite oder Anfrage[149].

136 Vgl. Hofer/Fischer (2010), S. 187.
137 Vgl. ebenda, S. 66.
138 Vgl. ebenda, S. 306-307.
139 Vgl. ebenda, S. 347.
140 Vgl. ebenda, S. 399.
141 Vgl. ebenda, S. 405.
142 Vgl. ebenda, S. 384.
143 Vgl. ebenda, S. 405.
144 Vgl. Schreiber/Schleier (2012): Whitepaper HTTP STRICT TRANSPORT SECURITY (HSTS), SecureNet GmbH, online verfügbar unter: https://www.mgm-sp.com/wp-content/uploads/HTTP_Strict_Transport_Security_HSTS_Whitepaper.pdf, Stand 08.08.2017, S. 3-4.
145 Vgl. Digitale Gesellschaft (2012): Wie das Internet funktioniert, online verfügbar unter: https://digitalegesellschaft.de/wp-content/uploads/2012/04/digiges_wie_das_internet_funktioniert.pdf, Stand 08.08.2017, S. 6.
146 Vgl. Hofer/Fischer (2010), S. 464.
147 Vgl. ebenda, S. 504.
148 Vgl. BSI (2016): G5.143 Man-in-the-Middle-Angriff, online verfügbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g05/g05143.html, Stand 08.08.2017.
149 Vgl. Hofer/Fischer (2010), S. 71-72.

Eine **Programmierschnittstelle (API, Application Programming Interface)** ermöglicht die Anbindung eines Programms. Sie beschreibt, wie die Anbindung zu programmieren und zu verwenden ist[150].

Ein **Server** ist ein Programm oder ein Prozess, der teilnehmenden Clients (s.o.) Daten oder Dienste bereitstellt[151]. Der Server erhält Anfragen (Requests) von den Clients und ist für deren Verarbeitung zuständig[152].

Bei einem **SSL-Stripping-Angriff** wird eine Weiterleitung zwischen verschiedenen Webseiten in der Art unterbunden, dass zwischen Nutzer und Anbieter kein verschlüsselter Kanal (HTTPS (s.o.)) aufgebaut wird. Die Kommunikation bleibt damit unverschlüsselt und beeinflussbar. Oftmals kann ein solcher Angriff am fehlenden Sicherheitsschloss in der Adresszeile des Browsers (s.o.) erkannt werden[153].

Ein (Security-)**Token** ist eine Komponente, die zur Identifizierung und Authentifizierung von Benutzern dient. Ein Token kann dabei verschiedenste Erscheinungsformen haben, wie z.B. als Smartcard in Form einer Karte, die dann ein Kartenlesegerät benötigt[154].

Transport Layer Security (TLS) ist ein Verschlüsselungsprotokoll. Es dient der sicheren Übertragung von Daten im Internet[155].

150 Vgl. ebenda, S. 45.
151 Vgl. ebenda, S. 805-806.
152 Vgl. ebenda, S. 170.
153 Vgl. Schreiber/Schleier (2012), S. 3-4.
154 Vgl. BSI Glossar, online verfügbar unter: https://www.bsi-fuer-buerger.de/SharedDocs/Glossareintraege/DE/T/Token.html, Stand 08.08.2017.
155 Vgl. BSI (2015b), S. 51.

9. QUELLENVERZEICHNIS

Amazon Pay (2017): Amazon Pay API reference guide, online verfügbar unter: https://pay.amazon.com/de/developer/documentation/apireference/201751630, Stand 07.08.2017.

Amazon Pay (2013): Datenschutzbestimmungen, online verfügbar unter: https://pay.amazon.com/de/help/201751600, Stand 22.07.2016.

Brettschneider, Frank/Haug, Oliver/Streiftau, Natalie/Wehner, Anja (2014): Für Kunden oft schwer zu verstehen: Die Sprache der Banken 2014, online verfügbar unter: https://komm.uni-hohenheim.de/uploads/media/2014-08-03_Bankenstudie_01.pdf, Stand 07.08.2017.

Bundesamt für Sicherheit und Informationstechnik (BSI) (2017a): BSI-TR-02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen; online verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf;jsessionid=CC1CBACBD558AC9AD3B6DC31C3E38979.2_cid360?__blob=publicationFile&v=4, Stand 07.08.2017.

Bundesamt für Sicherheit und Informationstechnik (BSI) (2017b): Glossar Token, online verfügbar unter: https://www.bsi-fuer-buerger.de/SharedDocs/Glossareintraege/DE/T/Token.html, Stand 07.08.2017.

Bundesamt für Sicherheit und Informationstechnik (BSI) (2016): G5.143 Man-in-the-Middle-Angriff, online verfügbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g05/g05143.html, Stand 07.08.2017.

Bundesamt für Sicherheit und Informationstechnik (BSI) (2015a): Empfehlung IT im Unternehmen. TLS/SSL Best Practice, online verfügbar unter: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_012.pdf;jsessionid=8F96D96295E8D67EF48F0074A01E8E51.1_cid369?__blob=publicationFile&v=4, Stand 07.08.2017.

Bundesamt für Sicherheit und Informationstechnik (BSI) (2015b): Die Lage der IT-Sicherheit in Deutschland, online verfügbar unter: https://www.bsi-fuer-buerger.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2015.pdf?__blob=publicationFile&v=5, Stand 07.08.2017.

Bundesamt für Sicherheit und Informationstechnik (BSI) (2014): M 2.488 Web-Tracking, online verfügbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02488.html, Stand 07.08.2017.

Bundesamt für Sicherheit und Informationstechnik (BSI) (2013): M 4.133 Geeignete Auswahl von Authentifikationsmechanismen, online verfügbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04133.html, Stand 07.08.2017

Bundesamt für Sicherheit und Informationstechnik (2007): Web 2.0, Sicherheitsaspekte neuer Anwendungen und Nutzungsformen des Mediums World Wide Web und ihrer Implementierung, online verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Web20/web20_pdf.pdf?__blob=publicationFile&v=2, Stand 07.08.2017.

Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) (2017): Datenschutzgrundverordnung, online verfügbar unter: https://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO6.pdf?__blob=publicationFile&v=24, Stand 08.08.2017.

Bundesministerium des Inneren (BMI) (2017): Ausweiskopien sind mit Einverständnis erlaubt, online verfügbar unter: http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Der-Personalausweis/Ausweis_kopieren/ausweis_kopieren_node.html, Stand 20.09.2017.

Christmann, Ursula/Groeben, Norbert (1996): Textverstehen/Textverständlichkeit - ein Forschungsüberblick unter Anwendungsperspektive, in: Krings, Hans (Hg.): Wissenschaftliche Grundlagen der Technischen Kommunikation, Gunter Narr Verlag Tübingen, S. 129-190.

Dapp, Thomas (2015): Fintech reloaded – Die Bank als digitales Ökosystem, Deutsche Bank, online verfügbar unter: https://www.dbresearch.de/PROD/RPS_DE-PROD/PROD0000000000443890/Fintech_reloaded_%E2%80%93_Die_Bank_als_digitales_%C3%96kosyste.pdf, Stand 07.08.2017.

Dautzenberg, Kirsti/Gaßmann, Constanze/Groß, Britta/Lambeck, Sebastian/Lück, Maike/Prüßner, Hannes (2017a): E-Payment – Bezahlen im Internet, Marktdynamik und Verbrauchersicht auf elektronische Bezahlverfahren im deutschen Internet-Handel, online verfügbar unter: http://www.marktwaechter.de/sites/default/files/downloads/untersuchungsbericht_marktwaechter_e-payment_pdf.pdf, Stand 07.08.2017.

Dautzenberg, Kirsti/Gaßmann, Constanze/Groß, Britta/Lambeck, Sebastian/Lück, Maike/Prüßner, Hannes (2017b): Nutzung elektronischer Bezahlsysteme: Werden Datenschutzbestimmungen vom Verbraucher gelesen?, online verfügbar unter: https://ssl.marktwaechter.de/sites/default/files/downloads/infografik-datenschutz-elektronische-bezahlsysteme.pdf, Stand 07.08.2017.

Digitale Gesellschaft (2012): Wie das Internet funktioniert, online verfügbar unter: https://digitalegesellschaft.de/wp-content/uploads/2012/04/digiges_wie_das_internet_funktioniert.pdf, Stand 07.08.2017.

Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI) (2015): Einkaufen in der digitalen Welt, online im Internet: https://www.divsi.de/wp-content/uploads/2015/08/2015-08-18-Online-Shopping_web.pdf, Stand 07.09.2017.

giropay (2017): GiroCheckout API, online verfügbar unter: http://api.girocheckout.de/girocheckout:giropay:start, Stand 07.08.2017.

Google (2017): CSP Evaluator, online verfügbar unter: https://csp-evaluator.withgoogle.com/, Stand 07.08.2017.

Hofer, Peter/Fischer, Peter (2010): Lexikon der Informatik, 15. Auflage, Springer.

Information Commissioner's Office (ico) (2017): Can I charge a fee for dealing with a subject access request?, online verfügbar unter: https://ico.org.uk/for-organisations/guide-to-data-protection/principle-6-rights/subject-access-request/, Stand 01.07.2017.

Kailas, Patil/Braun, Frederik (2016): A Measurement Study of the Content Security Policy on Real-Word Applications. International Journal of Network Security, Jg. 18, Nr.2, S. 383-392, online verfügbar unter: https://www.researchgate.net/publication/285218986_A_measurement_study_of_the_content_security_policy_on_real-world_applications, Stand 08.08.2017.

Linux Manpages Online (2017): sslscan, online verfügbar unter: https://man.cx/sslscan, Stand 07.08.2017.

McDonald, Aleecia/Cranor, Lorrie Faith (2008): The Cost of Reading Privacy Policies, online verfügbar unter: http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf, Stand 07.08.2017.

McDonald, Aleecia/Reeder, Robert/Kelley, Patrick/Cranor, Lorrie Faith (2009): A Comparative Study of Online Privacy Policies and Formats, in: Privacy Enhancing Technologies. PETS 2009. Lecture Notes in Computer Science. Jg. 5672. S. 37-55.

Mommers, Christian (2012): Nicht bemerkt?! Personalausweis kopieren verboten!, online verfügbar unter: https://www.datenschutzbeauftragter-info.de/nicht-bemerkt-personalausweis-kopieren-verboten/, Stand 07.08.2017.

National Institute of Standards and Technology (NIST) (2017): Digital Identity Guidelines, online verfügbar unter: https://pages.nist.gov/800-63-3/sp800-63b.html#sec7, Stand 07.08.2017.

National Institute of Standards and Technology (NIST) (2013): CVE-2013-6837 Detail, online verfügbar unter: https://nvd.nist.gov/vuln/detail/CVE-2013-6837, Stand 07.08.2017.

paydirekt (2017): REST-API, paydirekt – Version 1.5, online verfügbar unter: https://www.paydirekt.de/haendler/merchant-api.html, Stand 07.08.2017.

paydirekt (2016): Hinweise zum Datenschutz, online verfügbar unter: https://www.paydirekt.de/agb/index.html, Stand 27.07.2016.

PayPal (2017a): Payments API, online verfügbar unter: https://developer.paypal.com/docs/api/payments/, Stand 07.08.2017.

PayPal (2017b): PayPal-Datenschutzgrundsätze, online verfügbar unter: https://www.paypal.com/de/webapps/mpp/ua/privacy-full?locale.x=de_DE, Stand 01.07.2017.

Rohleder, Bernhard (2015): Datenschutz in der digitalen Welt, Bitkom, online verfügbar unter: https://www.bitkom.org/Presse/Anhaenge-an-PIs/2015/09-September/Bitkom-Charts-PK-Datenschutz-22092015-final.pdf, Stand 07.08.2017.

Schaar, Peter (2017): Verbraucherdatenschutz in der Digitalisierung, Herausforderungen und Lösungsansätze, Friedrich-Ebert-Stiftung, online verfügbar unter: http://library.fes.de/pdf-files/wiso/13497.pdf, Stand 07.08.2017.

Schneider, Markus/Enzmann, Matthias/Stopczynski, Martin (2014): Web-Tracking-Report 2014, Fraunhofer-Institut für sichere Informationstechnologie, online verfügbar unter: https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Web_Tracking_Report_2014.pdf?_=1422365497, Stand 07.08.2017.

Schreiber, Thomas/Schleier, Sven (2012): Whitepaper HTTP STRICT TRANSPORT SECURITY (HSTS), SecureNet GmbH, online verfügbar unter: https://www.mgm-sp.com/wp-content/uploads/HTTP_Strict_Transport_Security_HSTS_Whitepaper.pdf, Stand 07.08.2017.

Skrill (2017): Skrill Quick Checkout Integration Guide, online verfügbar unter: https://www.skrill.com/fileadmin/content/pdf/Skrill_Quick_Checkout_Guide.pdf, Stand 07.08.2017.

SOFORT GmbH (2017): SOFORT Überweisung – API Dokumentation, online verfügbar unter: https://www.sofort.com/integrationCenter-ger-DE/content/view/full/2513#hl, Stand 07.08.2017.

SOFORT GmbH (2015): Datenschutzhinweise, online verfügbar unter: https://documents.sofort.com/sue/datenschutzhinweise_ch, Stand 22.07.2016.

Verbraucherzentrale Bundesverband (vzbv): BGH stärkt Kundenrechte beim Bezahlen im Internet, online verfügbar unter: http://www.vzbv.de/pressemitteilung/bgh-staerkt-kundenrechte-beim-bezahlen-im-internet, Stand 08.08.2017.

Gesetzestexte

Bürgerliches Gesetzbuch (BGB), online verfügbar unter: https://www.gesetze-im-internet.de/bgb/BJNR001950896.html, Stand 07.08.2017.

Bundesdatenschutzgesetz (BDSG), online verfügbar unter: https://www.gesetze-im-internet.de/bdsg_1990/BJNR029550990.html, Stand 07.08.2017.

Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG), online verfügbar unter: https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html, Stand 07.08.2017.

Grundgesetz für die Bundesrepublik Deutschland (GG), online verfügbar unter: https://www.gesetze-im-internet.de/gg/BJNR000010949.html, Stand 07.08.2017.

Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, online verfügbar unter: http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:31995L0046&from=DE, Stand 07.08.2017.

Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, online verfügbar unter: http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016L0680&from=DE, Stand 07.08.2017.

Telemediengesetz (TMG), online verfügbar unter: https://www.gesetze-im-internet.de/tmg/BJNR017910007.html, Stand 07.08.2017.

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 (DGSVO), online verfügbar unter: http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679&from=DE, Stand 07.08.2017.

Kommentare

Gola, Peter/Klug, Christoph/Körffer, Barbara (2015): Bundesdatenschutzgesetz, 12. Auflage, C.H.Beck, abgerufen von: https://beck-online.beck.de.

Habel, Oliver/Müller, Eckart (2017), in: Forgó, Nikolaus/Helfrich, Marcus/Schneider, Jochen (Hg.): Betrieblicher Datenschutz, 2. Auflage, C.H.Beck.

Jandt, Silke/Schaar, Peter/Schulz, Wolfgang (2013), in Roßnagel, Alexander (Hg.): Beck'scher Kommentar zum Recht der Telemediendienste, 1. Auflage, C.H.Beck.

Müller-Broich, Jan (2012): Telemediengesetz, 1. Auflage, Nomos, abgerufen von: https://beck-online.beck.de.

Nink, Judith/Spindler, Gerald (2015), in: Spindler, Gerald/Schuster, Fabian (Hg.): Recht der elektronischen Medien, 3. Auflage, C.H.Beck, abgerufen von: https://beck-online.beck.de.

Schild, Hans Hermann (2017), in: Wolff, Amadeus/Brink, Stefan (Hg.): BeckOK Datenschutzrecht, 20. Auflage, C.H.Beck, abgerufen von: https://beck-online.beck.de.

Schröder, Georg (2016): Datenschutzrecht für die Praxis, 2. Auflage, dtv, abgerufen von: https://beck-online.beck.de.

Worms, Christoph (2017), in: Wolff, Amadeus/Brink, Stefan (Hg.): BeckOK Datenschutzrecht, 20. Auflage, C.H.Beck, abgerufen von: https://beck-online.beck.de.

Urteile

Bundesverfassungsgericht (BVerfG), Urteil vom 15. September 1983, AZ 1 BvR 209/83.

IMPRESSUM

Herausgeber
Verbraucherzentrale Brandenburg e. V.
Geschäftsführer Dr. Christian A. Rumpke
Babelsberger Str. 12
14473 Potsdam
Tel. (0331) 298 71-0
Fax (0331) 298 71-77
E-Mail marktwaechter@vzb.de

Autoren: Dr. Kirsti Dautzenberg, Constanze Gaßmann, Britta Groß, Sebastian Lambeck, Maike Lück, Hannes Prüßner

Titelbild: shutterstock/VectorHot
Gestaltung: Henrike Ott, Visuelle Kommunikation
Druck: Königsdruck – Printmedien und digitale Dienste GmbH

Stand: November 2017
Gedruckt auf 100 Prozent Recyclingpapier

Gefördert durch:

Bundesministerium der Justiz und für Verbraucherschutz

aufgrund eines Beschlusses des Deutschen Bundestages

verbraucherzentrale