



Datenschutz als Herausforderung für die Digitalisierung

Mai 2022 | Studie zur Evaluierung von Anwendungsfällen von Datenschutzhürden in Europa mit Schwerpunkt Deutschland

Inhalt

- 1 Zielsetzung und Grundlagen
- 2 Methodik
- 3 Ergebnisübersicht
- 4 Überblick zur DS-GVO
- 5 Branchenüberblick und Anwendungsfälle
- 6 Limitationen und Bibliographie

01

Zielsetzung und Grundlagen

Zielsetzung und Grundlagen

Ausgangslage

Nationale und internationale Regulierungen zum Datenschutz haben Unternehmen in den letzten Jahren vor große Herausforderungen zur Einhaltung der strengen Bestimmungen gestellt.

Wie eine aktuelle Erhebung des Bitkom aufzeigt, sind dabei die größten Probleme nach wie vor die weiter zunehmende Rechtsunsicherheit (78%), immer neuen Anforderungen (74%), mangelnden Umsetzungshilfen durch die Aufsichtsbehörden (66%) und uneinheitlichen Auslegungen der Bestimmungen innerhalb der Europäischen Union (52%).¹ Besonders schwer mit der Umsetzung tun sich dabei kleine und mittelständische Unternehmen. Alarmierend ist aber vor allem auch die Feststellung, dass aufgrund der DS-GVO oder damit verbundener Rechtsunsicherheit Innovationsprojekte scheitern. Nach Aussagen des BMWK und Erhebungen der KfW-ifo sind zudem die Investitionen des Mittelstandes als stärkstem Innovationsmotors Deutschlands in Forschung und Entwicklung mit insgesamt minus 6,3% stark rückläufig im Vergleich der Jahre 2021 und 2020.² Zudem hinkt Deutschland im internationalen Vergleich hinterher.³ Eine Schwächung der Innovationskraft hat also direkte Auswirkungen auf die zukünftige Wirtschaftskraft und -entwicklung. Daher ist es besonders wichtig, Barrieren für Innovation zu erkennen und diesen zielgerichtet entgegenzuwirken.

Zielsetzung und Grundlagen

Ziel der Studie

Die deutsche Politik unternimmt mit Förderprogrammen Anstrengungen, die Innovationskraft wieder zu stärken. Dabei ist es besonders wichtig, auch gegenläufige Faktoren zu beseitigen, um eine optimale Wirkung dieser Programme zu erzielen.

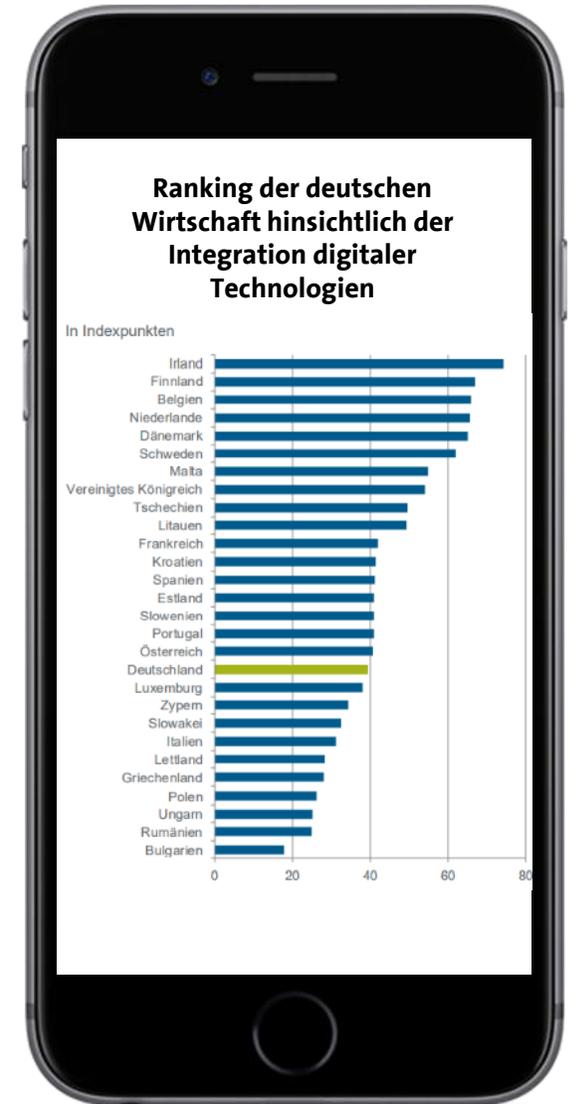
Ziel dieser Studie ist es, anhand von konkreten Beispielen, Innovations- und Digitalisierungsbarrieren aufgrund der DS-GVO aufzuzeigen und zu bewerten. Daraus können Vorschläge und Maßnahmen abgeleitet werden, die dem erkennbaren Trend entgegenwirken und die wirtschaftliche Entwicklung der deutschen Wirtschaft stärken, sowie Wettbewerbsnachteile beseitigen. Sie soll die Ergebnisse der von Bitkom erstellten Erhebung weiter vertiefen, um konkrete Argumente und Handlungsvorschläge abzuleiten. Zudem sollen Wettbewerbsnachteile im internationalen Vergleich sichtbar gemacht und konkretisiert werden.

↗Bitkom-Studie:
Gründe für Probleme

In **76%** der Unternehmen ist mindestens ein Innovationsprojekt aufgrund konkreter Vorgaben der DS-GVO gescheitert.

In **86%** der Unternehmen ist mindestens ein Innovationsprojekt aufgrund von Unklarheiten im Umgang mit der DS-GVO gescheitert.

↗Chart: BMWK Deutschland
im internationalen Vergleich
nur auf Platz 18



02

Methodik

Methodik

Unser Ansatz



- Kundenbefragung in Deutschland und Europa
- Befragung innerhalb von Accenture
- Erhebung von Marktdaten



Methodik

Schlüsselfragen an Interviewees

Allgemeine Fragen

- Beschreiben Sie Ihre Rolle, technischen Hintergrund und Branchenfokus.
- Bitte beschreiben Sie Ihre aktuellen Projekte.
- Welche Daten sind involviert?
- Auf welche Regelungen sind Sie gestoßen?
- Sind Sie auf die Situation gestoßen, dass Sie mit einer Idee oder einem Projekt nicht weitergekommen sind?

Spezielle Fragen

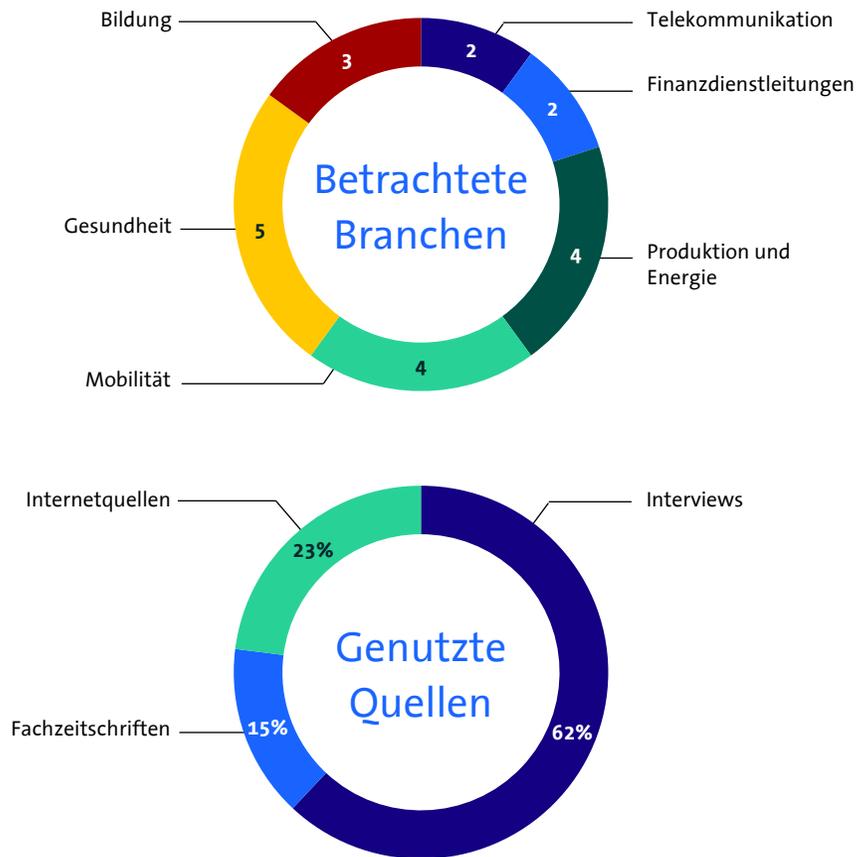
- Was sind die detaillierten Bedenken, die Sie identifiziert haben? Bitte um Beispiele.
- Wie konnten Sie die Bedenken überwinden?
- Wie war die Lösungsstrategie?
- Was haben Sie zu Beginn des Projekts unternommen, um das Thema konkreter zu gestalten und Gerüchte zu reduzieren?
- Kennen Sie Kosten, Markt, Zeitaufwand, Ressourcen in Verbindung mit Datenschutzbedenken am Projekt?

Finale Fragen

- In welchen Bereichen hat die Datenschutz Ihrer Meinung nach den größten Einfluss?
- Welche Verbesserungen sehen Sie? Was könnte geändert werden?

Methodik

Auswertung



Es werden Primärdaten erhoben und ausgewertet sowie Sekundärdaten verwendet und aktualisiert. Bei der Auswahl wird, wenn möglich, auf eine gleichmäßige Verteilung über die Industrien, Branchen, etc. geachtet, wobei aufgrund der kurzfristigen Beauftragung der Studie sowie der Durchführung der Studien in der Urlaubszeit nur eine limitierte Auswahl besteht.

Datengrundlage der Studie ist,

einerseits die **Erhebung von Primärdaten und anonymisierte Auswertung** der geführten Protokolle von Befragungen, Diskussionsrunden, etc. (aus kurzfristig verfügbaren eigenen, Accenture-internen/externen Kontakten), andererseits, die **Aktualisierung und Überarbeitung von Sekundärdaten** von internem Accenture-Material sowie öffentlich zugänglichen Studien

Je nach Verfügbarkeit, **Ergänzung der Daten, um Informationen, die durch Bitkom-Mitglieder/Kunden** bereitgestellt werden.

03

Ergebnisübersicht

Wichtigste Erkenntnisse

Datenschutz wird nicht in Frage gestellt, doch zeigt unsere Statuserhebung auch große Herausforderungen für Unternehmen.



Bedürfnisse für innovative, benutzerfreundliche Produktions- & Entwicklungsprozesse aus der Praxis stimmen oft nicht mit formalistischen Datenschutzregelungen überein.



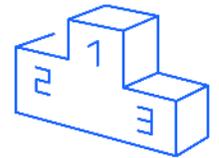
Ständige Nachbesserungen von Datenschutzregelungen führen dazu, dass Unternehmen mit Änderungen nicht mithalten können und mit veralteten Prozessen und Informationen arbeiten.



Aufgrund vieler juristischer Regelungen kann keine stabile Lieferkette hergestellt werden.



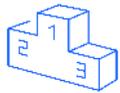
Langwierige Aufklärungsprozesse zu Fragen bezüglich DS-GVO-Anforderungen führen zu erheblichen Verzögerungen bei Innovationsprojekten.



Hohe Anforderungen an DS-GVO führen zu Einschränkung der Flexibilität von Unternehmen bei der Wahl von Service-Partnern und dadurch zu Wettbewerbsverzerrungen.

Ergebnisübersicht

Die Bedeutung von Datenschutz bleibt unbestritten, doch sind die unsichere Rechtslage, aber auch hohe technische und organisatorische Kosten, die größten Herausforderungen.



Hohe Anforderungen an DS-GVO führen zu Einschränkung der Flexibilität von Unternehmen bei der Wahl von Service-Partnern und dadurch zu Wettbewerbsverzerrungen, insbesondere im internationalen Vergleich.



DS-GVO-Anforderungen führen zu höheren Servicekosten, die erzielbare Margen mindern, Geschäftsmodelle gefährden und sogar Wettbewerbsnachteile schaffen.



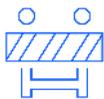
Rechtsunsicherheiten beschränken Unternehmen beim Einsatz neuer innovativer Technologien wie AI, Cloud-Transformationen oder bei der Vernetzung von Anwendungen.



Kosten für DS-GVO-Anpassungen werden speziell von KMUs bei der Planung neuer Geschäftsmodelle nur wenig berücksichtigt und führen dadurch häufig zu Problemen bei der Umsetzung.



DS-GVO-Anforderungen führen zu Einschränkungen bei der Leistungsfähigkeit von digitalen Anwendungen insbesondere im Gesundheitswesen.



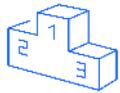
Hohe Kosten sowie technische und organisatorische Einschränkungen bei der Umsetzbarkeit von DS-GVO-Anforderungen führen zum Stopp von Digitalisierungsprojekten.



Langwierige Aufklärungsprozesse zu Fragen bezüglich DS-GVO-Anforderungen führen zu erheblichen Verzögerungen bei Innovationsprojekten.

Handlungsempfehlungen

Der Datenschutzrahmen bedarf zahlreicher Anpassungen.



Um Deutschland zum führenden Daten- und Digitalstandort zu entwickeln, bedarf es harmonisierter Auslegung und einer Umstrukturierung der Aufsichtsbehörden mit einheitlichen Anlaufstellen und Schwerpunktaufsichten.



Der Kostensteigerung für DS-GVO Compliance muss durch umfassende Beratungsangebote der Datenschutzaufsichtsbehörden Abhilfe geschaffen werden.



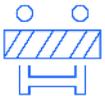
Rechtsunsicherheiten beim Einsatz neuer Technologien müssen minimiert werden. Hierfür müssen neue, klare Verarbeitungstatsbestände, auch in neuen Verordnungen wie dem EU Data Act und dem EU AI Act geschaffen werden.



KMUs sollten dezidierte Unterstützung erhalten, um datengetriebene Innovationen nicht länger zu verhindern.



Im Gesundheitsbereich sollten förderale Sonderregelungen abgeschafft beziehungsweise angeglichen werden.



Deutschland sollte sich für stärkere Harmonisierung und einen kohärenten Rechtsrahmen in Europa einsetzen, um die Wettbewerbsverzerrung durch unterschiedliche Anforderungen zu minimieren.



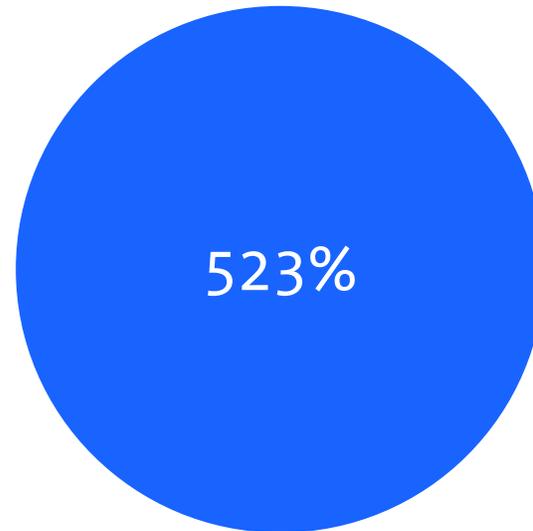
Das Dateninstitut sollte zu Datenkooperationen und Datenteilungsfragen beraten sowie den Aufbau von Kompetenzen fördern, zum Beispiel durch die Ausbildung von Data Scientists.

Zahlen und Fakten

DS-GVO und Schrems II schaffen Unsicherheit bei Unternehmen.
Eine Klärung wäre dringend nötig!



Bedenken hinsichtlich der Datensouveränität/Rechtsvorschriften gehören zu den größten Problemen bei der Cloud-Einführung
[Accenture. \(2021\). Keys to Cloud Continuum Success](#)



Erheblicher **Anstieg von Strafen** in 2021 im Vergleich zu 2020 – etwa 90 Mio Euro
[CMS. \(2021\). DS-GVO Enforcement Tracker](#)



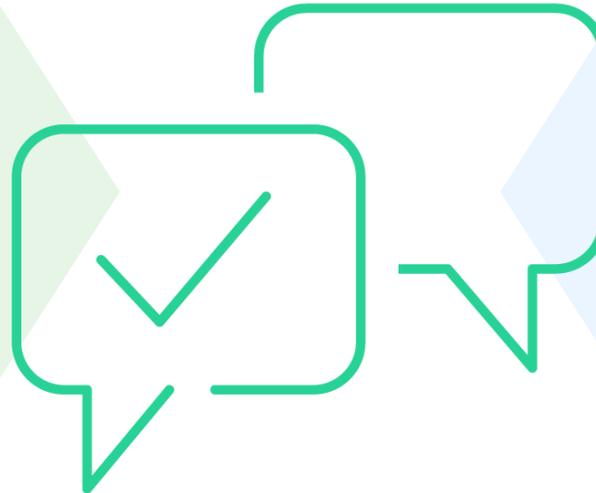
Ein Großteil der Unternehmen sieht **Rechtsunsicherheit** bei der Umsetzung der DS-GVO als größte Herausforderung
[Bitkom. \(2021\). Datenschutz als Daueraufgabe für die Wirtschaft](#)

Wie beeinflusst Datenschutz Innovationen?

Diskussion über die zwei Ansichten über Datenschutzerfordernissen und deren Einfluss auf Innovationen

Datenschutz bietet einen Rahmen für Innovationen

- Transparenz der Datennutzung
- Schutz der Privatsphäre und Betroffenenrechte
- Sichere Nutzung von Daten
- Indirekte Innovation neuer technischer Lösungen wie PKI, CMP, PIMS



Datenschutz schränkt innovative Projekte ein

- Rechtsunsicherheit
- Begrenzt technische Möglichkeiten
- Mehr Budget und Zeit erforderlich
- Unzureichende Ressourcen
- Begrenzt den Wettbewerb

Vielfältige Sichtweisen

„Datenschutz ist notwendig für Nachhaltigkeit.“

Beraterin für IT Sicherheit

„Kosten und Zeitaufwand für die Umsetzung sind zu hoch, um sie aufrechtzuerhalten.“

KMU-Eigentümer

„Der Produktsektor ist weniger reguliert und entsprechend zögert er weniger bei der Nutzung von Cloud-Lösungen.“

Managerin für IT Sicherheit

„Zu viel Regulierung beeinträchtigt die Wettbewerbsfähigkeit.“

Verkaufsberater

„Eine gesunde Sicherheitskultur ist fundamental.“

Lösungsarchitekt

„DS-GVO ist ein Hindernis für Innovationen im Hinblick auf personalisierte Kundenlösungen.“

Wirtschaftsanalystin

„DS-GVO schränkt Innovation nicht ein.“
„Es gibt immer einen Weg, Hürden zu umgehen.“

AI-Ingenieur

„Die Kluft zwischen Datenschutz und Technologie ist riesig.“

Lösungsarchitektin

Die Notwendigkeit der DS-GVO wird nicht in Frage gestellt, es braucht aber **Rechtssicherheit und leistbare, praktische Lösungskonzepte.**

Künstliche Intelligenz: Potenzial und Gefahr

KI erfordert ein hohes Maß an Datensicherheit, Datenschutz, und Datenbewusstsein. Die regulatorische Landschaft verändert sich kontinuierlich, sodass Rechtsunsicherheit bezüglich Do's and Dont's sowohl für Enterprises als auch KMUs eine große Herausforderung darstellt. KI gehört zu den Schlüsseltechnologien des 21. Jahrhunderts.¹

Herausforderungen

- 37% der Unternehmen sehen Fragen des Datenschutzes und 34% fehlenden Zugang zu externen Daten als große Herausforderung²
- Bereitschaft, Daten zu teilen, basiert auf dem Vertrauen auf sichere Datenverarbeitung
- Sind Algorithmen der KI-Modelle transparent und nachvollziehbar, steht der Mensch im Mittelpunkt?
- Herausfordernd sind fehlende Ressourcen & resultierende Kosten¹

Highlights

- Masking von Daten in der datenbasierten Wertschöpfungskette führt zu zusätzlichen Kosten und verminderter Datenqualität
- Kein Outsourcing außerhalb der EU, daher sorgfältige Webhosterauswahl
- Big Data-Analysen von Verhaltensmustern sind gängige Praxis

Anwendungsfälle



KI-Fahrerassistenz



Smart Meters



Voice- & Chatbots



Learning Analytics

04

Überblick zur DS-GVO

Übersicht der geregelten Themen der DS-GVO



Verarbeitungsverzeichnis & Rechenschaftspflicht

- Erfassung aller Verarbeitungstätigkeiten personenbezogener Daten inklusive Verwendungszweck, Speicherdauer, Kategorie betroffener Personen und Empfänger, etc.
- Dokumentation sämtlicher techn. und org. Maßnahmen (TOMs)



Rechtmäßigkeit & Einwilligungen

- Rechtsgrundlagen erfassen
- Datenminimierung beachten
- Konforme Einwilligungserklärungen einholen/dokumentieren/verwalten (wo notwendig)



Transparenz

- Erfüllung des Grundsatzes der Transparenz durch vollständige Datenschutzerklärungen in präziser, leicht zugänglicher Form in klarer und einfacher Sprache



Betroffenenrechte

Prozesse und technische Voraussetzungen für die Erfüllung von Betroffenenrechten sind zu schaffen:

- Auskunft
- Berichtigung
- Löschung und Einschränkung der Verarbeitung
- Datenportabilität



Sicherheit der Verarbeitung & Privacy by Design/Default

- Risiko-Analyse (ggf. Datenschutzfolgenabschätzung) und risikobasierte Auswahl geeigneter Schutzmaßnahmen zur Wahrung von
- Vertraulichkeit
 - Integrität
 - Verfügbarkeit



Datenpannenprozess

- Einrichtung geeigneter technischer und organisatorischer Maßnahmen zur Erkennung von Datenpannen und Prozesse, um innerhalb von 72h nach Erkennen reagieren zu können
- Meldung an die Behörde
 - Ggf. Mitteilung an betroffene Person
 - Dokumentation



Transfer & Auftragsverarbeiterverträge

- Abschließen von Auftragsverarbeiterverträgen
- Audit von Auftragsverarbeitern
- Geeignete Garantien bei Transfer in Drittländer



Speicherbegrenzung & Löschung

- Bildung von Datenarten
- Erhebung der Löschfristen
- Abhängigkeiten zwischen Systemen
- Technische Umsetzung der Löschung



DPO/DSB & Data Governance

- Klare Rollen, Zuständigkeiten und Verantwortung
- Steuerungsgremien- und Instrumente
- Richtlinien und Standards
- Training und Befähigung aller Beteiligten

Wichtige Artikel der DS-GVO

Von Auskunftsrecht bis hin zum Grundsatz der Datenminimierung

DatenSchutz-GrundVerordnung

RICHTLINIE ≠ **VERORDNUNG**
95/46/EG 2016/679
+ Nat. Recht

PERSONENBEZOGENE DATEN 1 & 4
„normal“ besondere Kategorien 9 strafrechtliche Verurteilungen 10
politische Meinungen
rassische oder ethnische Herkunft
religiöse oder weltanschauliche Überzeugungen,
sexuelle Orientierung, Gesundheits-, genetische,
biometrische Daten

Sachlich 2 **Räumlich** 3
natürlich juristisch ANWENDUNGS-
BEREICH EU

GRUNDSÄTZE 5 **RECHTMÄSSIGKEIT** 6

1) Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz	1) Einwilligung 7 & 8.	> freiwillig gegeben > in informierter Weise > für den konkreten Fall > unmissverständlich
2) Zweckbindung	2) Vertrag	> Für Kinder: Zustimmung der Eltern
3) Datenminimierung	3) Rechtliche Verpflichtung	
4) Richtigkeit	4) Lebenswichtige Interessen	
5) Speicherbegrenzung	5) Öffentliches Interesse	
6) Integrität und Vertraulichkeit	6) Berechtigtes Interesse	

Rechenschaftspflicht
*DSGVO Artikel

RECHTE DER BETROFFENEN PERSON

> Transparente Information 12
> knapp
> einfache Sprache
> verständlich
> leicht zugänglich
> transparent

Daten bei der betroffenen Person 13
> warum
> was
> wem
> Drittland -> Garantien
> wie lange
> welche Rechte
> vertraglich vorgeschrieben
> automatisierte Entscheidung + Logik
> andere Zwecke

> Bereitgestellte Information
Daten nicht bei der betroffenen Person 14

> Auskunft 15
> Berichtigung 16
> Löschung = Recht auf Vergessenwerden 17
> Einschränkung 18
> Datenübertragbarkeit 20
> Widerspruch 21
> Automatisierte Entscheidungen/Profiling 22

> Beschränkungen 23

Mitteilungs-
pflicht 19

DSGVO Artikel

VERANTWORTLICHER & AUFTRAGSVERARBEITER

> TOMs Verantwortlicher 24

> **Datenschutz durch Technikgestaltung** und durch datenschutzfreundliche Voreinstellungen 25
> zum Zeitpunkt der Festlegung der Mittel
> zum Zeitpunkt der eigentlichen Verarbeitung
> Im Einklang mit den Grundsätzen
> Im Einklang mit den Rechten der betroffenen Personen

> Gemeinsam für die Verarbeitung Verantwortliche 26
> Vereinbarung notwendig
> Transparenz für betroffene Personen

> Vertreter in EU 27

> **Auftragsverarbeiter (Vertrag) 28**
> Auftragsverarbeiter braucht Anweisungen des Verantwortlichen 29

> **Verzeichnis von Verarbeitungstätigkeiten 30**
> Zusammenarbeit mit der Behörde 31

> **Sicherheit der Verarbeitung 32**
> **Data Breach Notification 33** binnen 72 Stunden
> Data Breach Benachrichtigung an betroffene Personen 34

> Datenschutz-Folgenabschätzung 35/36
> neue Technologie
> umfangreiche sensible Daten
> systemat. Profiling
> Überwachung öffentlicher Plätze

> Datenschutzbeauftragter 37-39
> Verhaltensregeln 40/41
> Zertifizierung 42/43

ÜBERMITTLUNGEN AN DRITTLÄNDER 44-50

Hohe Regelungsdichte

Neben der DS-GVO gibt es noch weitere wichtige Gesetze zum Datenschutzrecht.



„Die Datenschutz-Grundverordnung (DS-GVO)¹ ist eine europäische Verordnung der Europäischen Union, seit 25. Mai 2018 die Grundlage des allgemeinen Datenschutzrechts in der EU, und regelt die Verarbeitung personenbezogener Daten von EU-Bürgern, unabhängig von der Ansässigkeit des verarbeitenden Unternehmens.“

Europäische Verordnungen und Richtlinien:

- Datenschutz-Grundverordnung (EU) 2016/679
- Data Governance Gesetz (EU) 2020/767
- Datenschutz-Richtlinie für den Bereich Justiz und Inneres (EU) 2016/680
- ePrivacy-Richtlinie (RL) 2002/58/EG

Europäische branchenspezifische Sonderregeln:

- Governance-Verordnung (EU) 2018/1999

Lokale Datenschutzgesetze:

- Bundesdatenschutzgesetz (BDSG)
- Bayerisches Datenschutzgesetz (BayDSG)
- Landesdatenschutzgesetz (LDSG) von Schleswig-Holstein

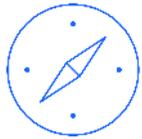
Lokale branchenspezifische Sonderregeln:

- IT-Sicherheitsgesetz 2.0 (ITSiG)
- Telekommunikationsgesetz (TKG)
- Telekommunikations-Telemedien-Datenschutzgesetz (TTDSG)

Lokale Landesgesetze:

- Gesundheitsschutzgesetz (GSG) von Bayern
- Landesgesundheitsgesetz (LGG) von Baden-Württemberg

Datentransfers außerhalb der EU/des EWR bedürfen zusätzlicher Aufmerksamkeit



Herausforderung

Die Hauptsitze der größten Cloud-Anbieter befinden sich in den USA. Die Anforderungen aus lokalen Gesetzen wie DS-GVO und Cloud Act haben einen großen Einfluss.



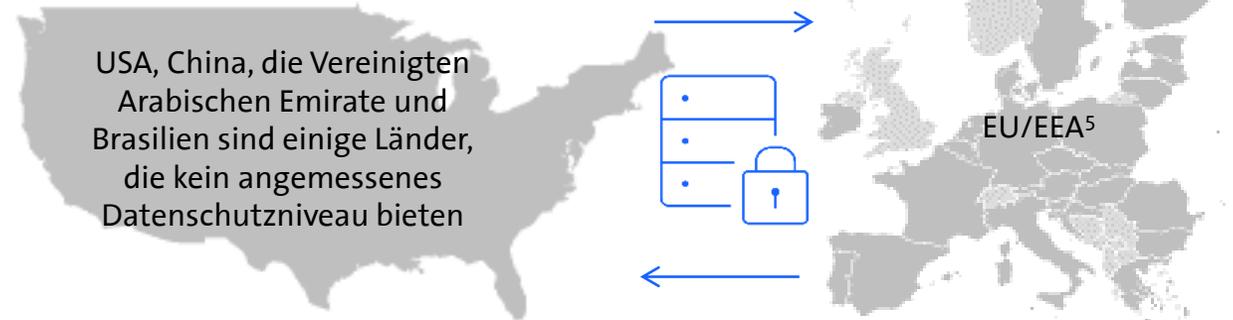
Schrems II Urteil

Das „Privacy Shield“ als Mechanismus für die Übertragung von Daten zwischen EU und US wurde für unwirksam erklärt und neue Anforderungen an den Datentransfer definiert.¹



DS-GVO Anforderung

Eine Übermittlung personenbezogener Daten außerhalb der EU/des EWR darf nur vorgenommen werden, wenn ein angemessenes Schutzniveau geboten ist.²



Angemessenes
Datenschutzniveau
sicherstellen

NEWS

Wie jüngste nationale Entscheidungen zeigen, herrscht Rechtsunsicherheit bei der Nutzung von cloudbasierten Services :

- *deutsches Verwaltungsgericht verbietet Nutzung von US-Cookies³*
- *österreichische Datenschutzbehörde verbietet Google Analytics⁴*

Grund ist der Datentransfer in die USA.

Beispielhafte Übertragung personenbezogener Daten aus globaler Sicht

USA

In den USA gibt es noch kein Datenschutzgesetz auf Bundesebene. Der bundesstaatspezifische **CCPA** steht jedoch größtenteils im Einklang mit der **DS-GVO**, die den Verbraucherdatenschutz für Einwohner Kaliforniens anspricht. Für die Datenübertragung in die USA sind Garantien nach **Art. 46 DS-GVO** erforderlich.

Japan

Japans geändertes Datenschutzgesetz **APPI** tritt mit 2022 in Kraft. Japan erhielt einen Angemessenheitsbeschluss.

China

Der **PIPL** gilt extraterritorial für ausländische Unternehmen und Personen, die Daten von betroffenen Personen in China verarbeiten. Für die Datenübertragung nach China sind gemäß **DS-GVO Art. 46** Garantien erforderlich.

Australien

Das australische Datenschutzgesetz **Privacy Act 1988**, ergänzt durch weitere Gesetze wie dem **Privacy Amendment Act 2017**, enthalten eine Reihe von Datenschutzrechten, sogenannte **IPPs (Information Privacy Principles)**. Für die Datenübertragung nach Australien sind gemäß **DS-GVO Art. 46** Garantien erforderlich.

Indien

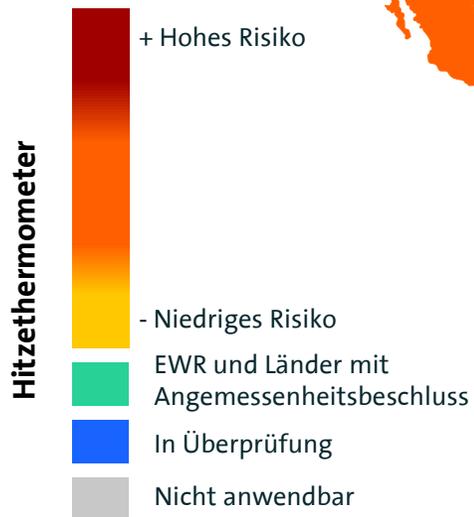
In Indien gibt es den **IT Act 2000** und die darin erlassenen datenschutzrechtlichen Vorschriften. Für die Datenübertragung nach Indien sind gemäß **DS-GVO Art. 46** angemessene Garantien erforderlich.

Südafrika

Südafrikas **POPI** ist strenger als die **DS-GVO**, da es für Informationen gilt, die über natürliche als auch juristische Personen erhoben werden. Für die Datenübertragung nach Südafrika sind Garantien gemäß **Art. 46 DS-GVO** erforderlich.

Brasilien

Brasiliens **LGPD** orientiert sich weitgehend an der **DS-GVO**. Für die Datenübertragung nach Brasilien sind Garantien gemäß **Art. 46 DS-GVO** erforderlich.



05

Branchenüberblick und Anwendungsfälle

Übersicht der betrachteten Branchen

Im Rahmen der vorliegenden Studie wurden Anwendungsfälle aus folgenden Branchen herangezogen



Mobilität

Im Verkehrskontext umfasst Mobilität die Autoindustrie, Luftfahrtindustrie sowie öffentliche Straßen und Verkehrsmittel.



Bildung

Die Bildungsbranche umfasst Bildungseinrichtungen von Schulen bis hin zu Universitäten und deren Nutzung von Services.



Finanzdienstleistungen

In die Finanzdienstleistungen fallen alle Dienstleistungen mit Bezug zu Finanzgeschäften, inklusive Banken, Finanzinstitute, Versicherungen.



Produktion und Energie

Die Produktions- und Energiebranche umfasst die Wertschöpfungskette von der Rohstoffgewinnung bis hin zur Energieversorgung.



Gesundheit

Gesundheitsbranche erfasst gesundheitsbezogene Applikationen, als auch Gesundheitsmanagement und Rettungsdienste.



Telekommunikation

Telekommunikationsunternehmen, kurz Telkos, bieten den Austausch von Informationen und Nachrichten durch ein Kommunikationssystem an.

Mobilität

2x

Doppelt so hohe Kosten für Etikettierung innerhalb der EU¹

14. Platz

Deutschland im Autonomous Vehicle Readiness index²

79.856.369€

Von der Gesamtsumme der im Transformations- & Energiesektor verhängten Geldbußen³



Die DS-GVO stellt Barrieren bei der Verbesserung und Erweiterung von Services auf, insbesondere bei der Anwendung neuer Technologien, wie AI und Cloud-Angeboten. Dazu gibt es viele unbegründete Vorwürfe, obwohl die Bestimmungen der DS-GVO eingehalten wurden. Dies deutet auf Rechtsunsicherheiten hin, die Unternehmen schon im Vorfeld von Innovationen abhalten.

Herausforderungen

- Neue Technologien der Digitalisierung, wie AI und Cloud-Lösungen, werden nur begrenzt eingesetzt
- Unterschiedliche nationale und internationale Bestimmungen führen zu Wettbewerbsverzerrungen
- Weiterentwicklungen der Geschäftsmodelle finden aufgrund von Rechtsunsicherheiten nicht statt

Highlights

- Unternehmen bieten einen eingeschränkten Funktionsumfang ihrer Services in DS-GVO-Regionen an
- Unterschiedliche Auslegung von DS-GVO führt zu unterschiedlichen Geschäftsmodellen in unterschiedlichen Regionen, auch innerhalb der EU

Anwendungsfälle



KI-Fahrassistenz



Personalisierte Preise



Risikoakzeptanz



Autonomes Fahren

Anwendungsfall

KI-Fahrerassistenz

Interview
mit der
Projektleitung



DS-GVO führt zu Anpassungen bei europäischen Fahrerassistenzlösungen, die künstliche Intelligenz nutzen.

Herausforderung

- Entwicklung von Software basierend auf KI/ML-Labeling-Technologie zur Gewährleistung der Fahrsicherheit
- Gesichtsmerkmale werden als personenbezogene Daten identifiziert, aber können nur erschwert nicht in die Labeling Labs in Indien oder China zur Verarbeitung übermittelt werden

Rechtlich

Datenübermittlung außerhalb der EU ist ohne rechtl. Grundlage unzulässig; DS-GVO Artikel 44 ff; C-311/18 (Schrems II)

Technisch

Aufbau von eigenen Labeling Labs (Etikettierlabor) und Projektneustart; alternativ Outsourcing innerhalb von Europa, falls verfügbar und leistbar.

Argumentation

Vision Engineer (Interviewee): Die Kosten für europäisches Labelling (Etikettierung) sind viel höher im Vergleich zu Indien oder China.

Projekte verzögerten sich, weil die Etikettierungslösung von Grund auf vor Ort innerhalb von Europa entwickelt werden musste.

Datenschutz hat für uns hohe Priorität. Es gibt für alles eine technische Lösung, aber das ist eher eine Kosten- und Zeitfrage.

B-plus automotive GmbH: Es ist herausfordernd, immense Datenmengen live zu verarbeiten, zu analysieren und zu speichern, um sie für das Trainieren neuer KI-Software und die Validierung neuer Fahrfunktionen zu verwenden.¹

BMVi: „Morgen tritt unser Gesetz zum autonomen Fahren in Kraft. Damit ist der Weg frei, um selbststeuernde Fahrzeuge ganz regulär auf die Straße zu holen – als erstes Land weltweit. Damit setzen wir internationale Standards.“²

Fazit

- Der Produktentwicklungsprozess musste neu begonnen werden, und ein Labelling Lab in der EU eingerichtet werden
- Diese DS-GVO-konforme Lösung erhöhte die Gesamtkosten und den Zeitaufwand
- Es besteht eine Kluft zwischen Politik, Technologie, und Recht im Bezug auf Wissensaustausch und Zusammenarbeit

Künstliche Intelligenz (KI, AI)

Wie lernt eine KI das Autofahren?

Selbstständig fahrende Autos müssen ihre Umgebung realitätsgetreu wahrnehmen. Das Start-up "understand.ai" erklärt, wie intelligente Algorithmen beim Labeling von Bild- und Videoaufnahmen lernen – und hat das Verfahren besser und schneller gemacht.

¹ Bayern innovative, Mit KI auf der Überholspur | ² BMVi, Gesetz zum autonomen Fahren

Quelle Screenshot: [Vision-mobility, Wie lernt eine KI](#)



Anwendungsfall

Personalisierte Preisgestaltung

Fluggesellschaften nutzen Cookies, um Flugpreise zu verfeinern. Dynamische Preisgestaltung ist bei der Preisgestaltung im Flugverkehr wie auch der Hotellerie und E-Commerce gängige Praxis. Der Einsatz individueller Preisgestaltung ist unklar.¹

Herausforderung

- Gerüchte über Preisänderungen bei Fluggesellschaften aufgrund der gesammelten Cookies
- Cookies werden zur Erstellung von Kundenprofilen gesammelt

Rechtlich

DS-GVO; E-Commerce Richtlinie; evtl. Digital Services Act & Digital Markets Act

Argumentation

BMJ-Studie: Die durchgeführte statistische Auswertung der Daten konnte nicht bestätigen, dass personalisierte Preisgestaltung im Markt vorliegt und von Anbietern aktiv eingesetzt wird. Dynamische Preisgestaltung ist gängige Praxis.¹

Airbnb: Wenn du die intelligente Preisgestaltung aktivierst, ändern sich Preise pro Nacht automatisch je nach Nachfrage, Art und Standort der Unterkunft, Jahreszeit, und anderen Faktoren.²

Staatssekretär Christian Kastrop zur BMJ-Studie: „Es ist rausgekommen, dass es im Moment so ist, dass es keine personalisierten Preise gibt aufgrund von Nutzerverhalten im Netz“.³

Fazit

- Fluggesellschaften sammeln Zustimmung für die Sammlung personenbezogener Daten aus Cookies
- Marketing-Cookies werden für die Erstellung von Kundenprofilen an Dritte für personalisierte Werbung & Marketing weitergegeben
- Keine Anhaltspunkte, dass sich der Preis durch die in Cookies gesammelten Informationen ändert. Auch lassen sich keine vergangenen DS-GVO-Bußgelder finden
- Personalisierte Preismodelle kaum reguliert



¹ ibi research, Schlussbericht, 72 | ² Airbnb, Hilfsartikel | ³ Deutschlandfunk, Studie zum Online-Handel

Quellen Screenshots: [FAZ, Keine personalisierten Preise](#); [help.ORF, Unterschiedliche Onlinepreise](#); [BMJ, Schlussbericht](#)

Anwendungsfall

DS-GVO: Risikoakzeptanz

Nicht-europäische Fluggesellschaft hinterfragt Anwendbarkeit und Durchsetzbarkeit der DS-GVO und trifft Entscheidung, das Risiko von DS-GVO-Bußgeldern bis zu einem gewissen Grad in Kauf zu nehmen.

Interview
mit der
Projektleitung



Herausforderung

- Bewertung der Einhaltung und möglichen Umsetzung der DS-GVO mittels Evaluierungsbericht und Implementierungsroadmap

Rechtlich

Artikel 32, 44 ff und 83 DS-GVO; C-311/18 (Schrems II)

Technisch

Implementierung diverser TOMs

Argumentation

Datenschutzberater: Jedes Unternehmen ist verpflichtet, angemessene Maßnahmen zum Schutz personenbezogener Daten zu treffen. Dafür eine Risikoanalyse durchzuführen, um entsprechend Maßnahmen zu treffen, wobei Auswahl sowie Art und Weise der Umsetzung einen Spielraum bieten.¹

Standard-Datenschutzmodell 2.0b: Risikoakzeptanz oder -transfer steht wie in der Informationssicherheit nicht zur Verfügung. Das Restrisiko muss angemessen sein.²

Datenschutzberater: Der Aufwand für eine solche Risikoanalyse ist nicht zu unterschätzen.¹

Dr. DS-GVO: Mailjet gibt an DS-GVO-konform zu sein und gleichzeitig wird angegeben, dass Daten in Rechenzentren mit Google Cloud Plattform in Frankfurt und Saint-Ghislain gespeichert werden.

Fazit

- Die Kosten für die Implementierung einer DS-GVO-konformen Lösung sind höher
- Unternehmen nahm nach einer Evaluierung und Risikoanalyse die Konsequenzen nach DS-GVO in Kauf. Grund sind die kostspieligen TOMs. So werden die Passagierdaten unter Umständen rechtsunsicher in Länder außerhalb der EU übertragen
- Aufgrund der unterschiedlichen Sichtweisen, können Betroffene nur schwer fundierte Entscheidungen treffen



¹ Bayern innovative, Mit KI auf der Überholspur | ² BMVI, Gesetz zum autonomen Fahren



Anwendungsfall

Autonomes Fahren

Die EU sucht nach einer Balance zwischen Datensicherheit, Datenschutz und Innovation. Aufgrund der ständigen neuen Regelungen bzw. Anpassungen bestehender Regelungen, müssen Unternehmen viel Aufwand, Budget und Ressourcen in die Hand nehmen, um den Anforderungen der DS-GVO gerecht zu werden.

Herausforderung

- (Voll-)autonomes Fahren benötigt eine kohärente Menge an Daten
- Personenbezogene Daten: Sensor- und Bilddaten, Fahrerpräferenzen, Login-Daten, Bewegungs- & Verhaltensmuster, Mobilitätsdaten wie Kfz-Kennzeichen
- Fahrassistenzsysteme wie Spurhalte-, Abstandsassistenten und Einparksysteme

Rechtlich

DS-GVO; UNECE WP.29; EU General Safety Regulation

Technisch

Autohersteller müssen technische Maßnahmen implementieren, u.a. automatisches Anonymisieren/Pseudonymisieren von Daten unbeteiligter Dritter, und für Training von KI-Modellen

Argumentation

Vorstandsvorsitzender der Daimler AG Källenius: „Wir machen das Fahren sicherer, vernetzter, transparenter. Ich kann individuelle Dienste ein- und ausschalten. Und wenn ich zum Beispiel kein Fahrzeug-Tracking möchte, kann ich das auch ausschalten. Dann bin ich privat.“¹

Continental Chef Setzer: „Datenverarbeitung auf Rädern müsse man mit klassischen Sicherheitssystemen wie einer Bremse zusammendenken.“¹

Entwicklungschef von Volkswagen Ulbrich: „Wir haben die Technologieoffenheit für uns beiseitegelegt und auf die E-Mobilität gesetzt.“¹

EU General Safety Regulation: Anwendbar ab 2022 Juli für alle Pkws mit Typgenehmigung in der EU; u.a. Blackbox für ereignisbezogene Datenaufzeichnung, Vorrichtung Alcolock, Müdigkeitswarner.²

Fachleute: Geforderte Sicherheitsausstattung bei Kleinwagen kostet etwa 1.000 € pro Kfz.²

Gartner: drahtlose Telematikgeräte und Black Box-Technologien verarbeiten Daten zu Instandhaltung Fahrzeugnutzung und Wartungsbedarf.³

Fazit

- Bekannte Autohersteller setzen statt auf Digitalisierung und Technologieoffenheit eher auf Implementierung von Datenschutzlösungen für Kundinnen und Kunden
- Die Diskrepanz zwischen der Verarbeitung von Datenmengen für KI-Modelle und Datenschutz im Auto steigt³
- Der Datenschutz wird immer mehr in Industriestandards einbezogen, u.a. auch in den TISAX

Bildung

65%
der Lehrkräfte fühlen
Sich bei
Datenschutzfragen nicht
ausreichend
unterstützt^{2,3}

33%
der deutschen
Schulen sind
digitale
Nachzügler^{2,3}

57%
der Unternehmen
produzieren e-Learning-
Inhalte selbst ohne einen
externen Dienstleister
einzusetzen⁴



Unterschiedliche Positionen der lokalen Datenschutzbehörden führen zu einer großen Unsicherheit bei allen betroffenen Beteiligten, Schülerinnen und Schülern, Eltern und Lehrkräften, aber auch bei Anbietern von e-Learning-Anwendungen. Fehlende Klarheit von Zuständigkeiten und Verantwortlichkeiten, langwierige Bewertungsprozesse und unklare Entscheidungsprozesse und Entscheidungsgrundlagen sind wesentliche Kernprobleme.

Herausforderungen

- Bildungsinformationen können personenbezogene Daten sein
- Cloud-basierte Angebote außerhalb der EU sind nur begrenzt nutzbar
- Verantwortlichkeiten sind nicht eindeutig geregelt, bspw. zwischen Anbietern und Behörden
- Zustimmungsprozess (Consent) für Anwendende nicht transparent
- Unterschiedliche Aussagen sowohl national, als auch EU-weit
- COVID-19 als bedeutender Trigger¹

Highlights

- Durch Datenschutzbehörden wurden schwere Bedenken bezüglich amerikanischen Anbietern geäußert
- Unterschiedliche Sichtweisen auf nationaler und internationaler Ebene

Anwendungsfälle



Learning Analytics



Office 365 an Schulen



Videokonferenzdienste in Schulen



Anwendungsfall

Learning Analytics im E-Learning

Learning Analytics-Technologien finden sich bereits in zahlreichen Lernmanagementsystemen wieder. Beispiele sind Moodle und iMOOC, wobei umfassende Pseudonymisierung nicht vollumfänglich gewährleistet werden kann und die Umgehung das vermeindliche Potenzial von Learning Analytics verpasst.¹

Herausforderung

- Ziel: Lernmuster erkennbar machen
- Verarbeitung sensibler Daten in digitaler Form aus dem Bildungskontext
- Verwendung von KI-Systemen erklärbar, transparent, & diskriminierungsfrei machen¹
- Hürden: Angst um die Privatsphäre⁹

Rechtlich

DS-GVO; Gesetze aus Bildungssektor; lokale Gesetze; Compliance RLs; Trusted Learning Analytics als Konzept für Ethik und Recht²; Governance Act; AI Act; Data, Digital Markets & Services Act

Technisch

Learning Analytics ist u.a. in digitalen Lernumgebungen eingebunden und analysiert sowie visualisiert in Echtzeit das Nutzerverhalten der Lernenden durch Datenspuren³

Argumentation

Europäisches Parlament: Innovationen im Bildungsbereich sind überfällig, wie die COVID-19 Pandemie und die darauf folgende Umstellung auf Online- und Fernunterricht gezeigt haben; KI-gesteuerte Bildungswerkzeuge wie solche zur Bewertung und Erkennung von Lernschwierigkeiten können die Qualität und Wirksamkeit des Online-Lernens verbessern.⁴

Center of Data Innovation: Hohe Kosten durch die Regulierung – das KI-Gesetz kostet die europäische Wirtschaft 31 Millionen Euro. KMUs, die Hochrisiko-KI-Anwendungen entwickeln, sollten mit 400.000 € und 20% Investitionsvolumen aufgrund von Compliance-Kosten rechnen.

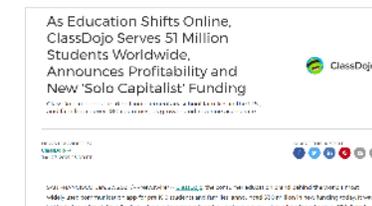
Rechtinformatik-Experte Borges: Die Gefahr einer Überregulierung und Belastung von Anbietern mit überhöhten Kosten für Risikomanagement besteht.⁵

Schulleiterin Winterhuder Reformschule: Es gilt immer wieder Datenschutz versus Funktionalität.⁶

Forscher des KIT: Aus der DS-GVO geht (jedoch) nicht eindeutig hervor, welche Arten von automatisierten Entscheidungen tatsächlich erfasst sind.⁷

Fazit

- Learning Analytics in Deutschland wenig eingesetzt, anders in den USA⁹
- Fehlende Arrondierung des Rechtsrahmens, daher Rechtsunsicherheit²
- Dies bedeutet, dass Rechtsfragen als Teil des Risikomanagements behandelt werden
- Aufgrund von den undurchsichtigen Sichtweisen, befinden sich Innovatoren im rechtsunsicheren Raum⁸



¹ Silvia Lipp, 129 | ² Silvia Lipp, 126 | ³ Silvia Lipp, 122 | ⁴ EP Bericht | ⁵ computerwelt, KI-Regulierung | ⁶ Forum Bildung Digitalisierung, Datenschutz | ⁷ GEW, Learning Analytics, 18 |

⁸ Bertelsmann Stiftung, KI in Unternehmen, 74 | ⁹ Elena Schmeing, 23-25 und 59

Anwendungsfall

Office 365 an Schulen

Marktforschung



In mehreren Bundesländern wird der Einsatz von Office 365 als Hilfsmittel für e-Learning vorbereitet. Aufgrund von fehlenden zentralen Vorgaben und Prüfungen besteht eine große Unsicherheit über die rechtlichen Konsequenzen sowohl von Verantwortlichen und Lehrpersonal wie auch von Eltern, Schülerinnen und Schülern.

Herausforderung

- Keine eindeutige Klärung, ob der Einsatz rechtskonform ist
- Lokale Lernmanagementsysteme sind nicht ausreichend
- Langwieriges Prüfverfahren
- Auswirkung auf andere Bereiche

Rechtlich

Artikel 12ff, 30, 35, 45 DS-GVO; C-311/18 (Schrems II); fehlende eindeutige Zuweisung der Verantwortlichkeiten

Technisch

Microsoft sammelt bei der Installation und im Betrieb Daten, die zur Ermittlung von Teilen des Nutzerverhaltens führen können, ohne das dafür explizit eine Einwilligung gegeben wurde.

Argumentation

Microsoft: Maßnahmen für den Schutz von Daten, sodass Kundinnen und Kunden weiter rechtskonform Microsoft-Dienste nutzen können.¹

Berliner DPA: Zusätzliche Maßnahmen sind nicht ausreichend, um das unzureichende Datenschutzniveau der USA auszugleichen.²

Ministerium Baden-Württemberg: Datenschutzkonforme Bildungsplattform kommt – nicht pauschal untersagt.³

Gutachten von DGC: Anbieter aus Drittstaaten wie aus den USA, aber auch aus China, erfüllen diese Voraussetzungen oft nicht.⁴

Bayerische DPA: Bei Office-Anwendungen außer der Videokonferenz kann Pseudonymisierung in Betracht kommen.⁵

Ministerium NRW: Empfiehlt „Logineo NRW“.⁶

Urteil des OLG Frankfurt: Schulen in Hessen dürfen Office 365 verwenden.⁷

Bezirksregierung Arnsberg: Nutzung von Google-Diensten in Schulen aufgrund von Elternbedenken verboten.⁸

Fazit

- Lokale Lösungen scheitern landesweit⁹
- Derzeit stufen diverse staatliche Stellen (BW, NRW, Berlin, Bayern) die Nutzung von MS Office 365 als bedenklich ein.^{2,3,6} Eine Prüfung ist sehr aufwendig und für die betroffenen Anwendergruppen intransparent
- Aufgrund der unterschiedlichen Sichtweisen können Betroffene nur schwer fundierte Entscheidungen treffen

Im Ergebnis empfiehlt der LfDI, von der Nutzung der erprobten MS-Produkte im Schulbereich abzusehen. Trotz des besonderten Zuspruchs der eingesetzten Produkte bleiben eine Vielzahl von Problemen und offenen Fragestellungen, welche weder das Kultusministerium noch die einzelnen Schulen datenschutzrechtlich verantworten können.

Die meisten Datenschutz-Verletzungen finden in der täglichen Schulverwaltung statt

Was sieht die datenschutzrechtliche Bewertung von Microsoft 365 für über schulischen Person/ in NRW aus?

Von der LfDI NRW ist mitgeteilt worden, dass ein bundesländerübergreifendes Verfahren zur datenschutzrechtlichen Beurteilung von Microsoft 365 stattfindet. Eine abschließende bundesländerübergreifende Bewertung der Datenschutzrisikoprüfung in Abstimmung mit Microsoft liegt noch nicht vor. Vor diesem Hintergrund wurde daher von der LfDI die Verarbeitung von personenbezogenen oder personenbezahbaren Daten innerhalb von Microsoft 365 aktuell als datenschutzrechtlich bedenklich eingestuft worden. Das Schulministerium empfiehlt daher, bei der Beschaffung und Nutzung von cloud-basierten Anwendungen auf die datenschutzliche Verfügbarkeit bedenkliche Angebote zu vermeiden. Für die Datenverarbeitung sind die DSGVO in NRW als Lernmanagementsystem sowie die DSGVO in NRW als Lernmanagementsystem mit integrierter Videokonferenzoption zur Verfügung zu stellen. Zudem ist die Nutzung der LfDI-LOGINEO NRW die Anbindung einer Office-Komponente vorgesehen.

1 Microsoft, Schrems II | 2 BlnBDI, Hinweise Berliner DPO | 3 KM-BW, digitale Bildungsplattform | 4 DGC Integrity, „Der Digitalpakt Schule“ | 5 BayLfD, Aktuelle Kurz-Information 39 |

6 Ministerium NRW, Fragen und Antworten | 7 dpa, Streit um Vergabe | 8 golem.de, Nutzung | 9 check.point, Lernmanagementsysteme

Quellen Screenshots: Fragdenstaat, 118410-2021-04-23 empfehlung lfdi; Schulministerium NRW, Fragen und Antworten zum Datenschutz; News4Teachers, Datenschutz an Schulen weitere Mythen

Anwendungsfall

Videokonferenzdienste

Treffende Datenschutzansichten bei Nutzung von cloudbasierten Diensten wie Zoom, Microsoft Teams, Google Meet, GoToMeeting, Skype, TeamViewer, Jitsi und Cisco Webex Meetings und lokale Ansätze wie LOGINEO NRW.

Marktforschung



Herausforderung

- Datentransfer an US-amerikanische Cloudanbieter
- Anbieter preisen DS-GVO-Konformität
- Datenschutzbehörden in Deutschland haben unterschiedliche Ansichten über rechtskonforme Nutzung der Dienste

Rechtlich

Artikel 45 DS-GVO; C-311/18 (Schrems II)

Technisch

Videokonferenzdienste stellen zwischen Personen eine visuelle Brücke in Echtzeit her. Dabei werden Cloud-basierende Technologien genutzt und es kommt zur Übertragung personenbezogener Nutzerdaten über das Internet zwischen mehreren Standorten.

Argumentation

HBDI: Erinnerung der hessischen Schullandschaft an das Auslaufen der Duldung bis 31. Juli 2021 von nicht datenschutzkonformen Videokonferenzsystemen.¹

Urteil des OLG Frankfurt: Vergabeverfahren wird gestoppt, folgend dürfen Schulen in Hessen Microsoft Teams weiterverwenden.²

Teamviewer-Sprecher: Damit können alle datenschutzrechtlichen Anforderungen der Kultusministerien in Deutschland, wie auch der europäischen Partnerländer, erfüllt werden.³

Kulturministerium Hessen: Die hessischen Schulen sollen ein einheitliches System für Videokonferenzen nutzen können, da die Schulen derzeit unterschiedliche Dienste nutzen.⁴

Ministerium NRW: Empfiehlt „Logineo NRW“.⁶

Gutachten von DGC: Anbieter aus Drittstaaten wie aus den USA, aber auch aus China, erfüllen DS-GVO Voraussetzungen oft nicht.⁵

Fazit

- Bildungseinrichtungen wie Schulen müssen auf alternative Videokonferenzdienste umsteigen, was Schulen Zeit und Geld kostet und dazu führt, dass gewisse Features nicht mehr genutzt werden können
- Aufgrund der unterschiedlichen Sichtweisen können Betroffene nur schwer fundierte Entscheidungen treffen



1 HBDI, Videokonferenzsysteme in Schulen | 2 ordentliche Gerichtsbarkeit Hessen Ausschreibung | 3 it-daily.net, Classroom-Lösung | 4 Frankfurter Allgemeine, Neue Ausschreibung | 5 DGC Integrity, Der Digitalpakt Schule | 6 Ministerium NRW, Fragen und Antworten
Quellen Screenshots: News4teachers, Datenschutz an Schulen; Das Windows 11 Magazin, Hessen Gerichtsurteil stoppt Verfahren

Finanzdienstleistungen

Jedem 8ten

Unternehmen fehlt es an konkreten Zielen bei der Implementierung innovativer Technologien¹

28.356.065€

Gesamtsumme der Geldbußen für Finanzen, Versicherungen und Beratung⁴

93

Gesamtanzahl der Geldbußen für Finanzen, Versicherungen und Beratung⁴



Die Finanzbranche stellt sich der Herausforderung der besonders hohen Regeldichte, gleichzeitig konzentrieren sich hier besonders viele Big Data-Projekte. Trotzdem kämpfen rund 48% der Unternehmen mit erforderlicher Datenqualität und Datensicherheit sowie 38% mit Komplexität und Nutzbarkeit.²

Herausforderungen

- Covid-19-Pandemie als Beschleuniger der Digitalisierung
- Hohe regulatorische und speziell branchenspezifische Vorgaben an Finanzinstitute und Banken
- Sicherheit, Datenschutz und Compliance haben oberste Priorität²
- Einsatz innovativer Technologien wie Cloud Computing und AI ist notwendig, um wettbewerbs-fähig zu bleiben
- Banken haben detaillierte Einblicke in das Leben ihrer Kunden³

Highlights

- Hohes Bewusstsein für Schutz von Kundendaten
- Die Unsicherheit bezüglich der Auslegung der DS-GVO kann Cloud-Projekte scheitern lassen
- Lokale Lösungen pro Land bzw. Markt aufgrund unvereinbarer Datenschutzgesetze
- Große rechtliche Unsicherheit bei Datensammlung und Auswertung von Big Data, Verstoß gegen Recht auf informationelle Selbstbestimmung möglich

Anwendungsfälle



Cloud Solution



Voice- & Chatbots

¹ Justus-Liebig-Universität Gießen; Chancen und Herausforderungen von Big Data, S 3; TechTarget, The Path to Data Leadership, S 7 | ² Microsoft, Microsoft Finanzmonitor |

³ staperior, DS-GVO und ihre Auswirkungen auf den Bankensektor | ⁴ CMS, GDPR Enforcement Tracker

Anwendungsfall

Zentrales Cloud Computing

Koreanisches Datenschutzgesetz (PIPA) sieht DS-GVO-Anforderungen als nicht ausreichend an und sieht strikere Anforderungen auch für Cloud Computing vor.

Interview
mit der
Projektleitung



Herausforderung

- Nichtübereinstimmung des koreanischen und europäischen Datenschutzrechts wurde zum Hindernis für ein Projekt über einen zentralisierten Cloud-Ansatz für eine globalen Verwaltung

Rechtlich

DS-GVO; PIPA (koreanisches Datenschutzgesetz)

Technisch

Koreanisches Datenschutzgesetz sieht zusätzliche 50 Anforderungen, u.a. striktes Logging auch von einzelnen Lesezugriffen, vor. Dieses ist bei einem globalen System aus technischer Sicht nicht performant.

Argumentation

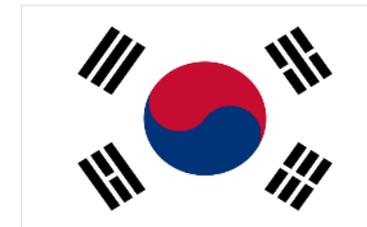
Projektleitung Interviewee: Motivation und Ansatz zur Umsetzung von Datenschutzregularien hängt von der Industrie ab.

Während die Pharmabranche Qualitätssicherung an erster Stelle sieht, priorisiert die Produktionsbranche nach Kritikalität und die Finanzdienstleistungsanbieter haben Verständnis und Awareness für Security und Privacy-Anforderungen.

Jedes Land hat eigene Anforderungen. Russland setzt bspw. immer voraus, eine unverschlüsselte Kopie in Russland zu belassen, während China sogar verlangt, dass eine lokale Kopie auf chinesischen Servern gespeichert werden muss.

Fazit

- Es war nicht möglich, die Geschäftsidee einer zentralen Cloud-Lösung umzusetzen. Es wurde eine eigene Cloud-Lösung entwickelt, nur für den koreanischen Markt
- Aufgrund der unterschiedlichen länderspezifischen Datenschutzgesetze musste das Projekt abgebrochen werden



Anwendungsfall

Voice- und Chatbots

Großbank baut, integriert und bettet einen Voice- und Chatbot auf deren Website für potenzielle und bestehende Bankkunden ein, um Digitalisierung voranzutreiben. DS-GVO-Anforderungen für Sammlung und Verarbeitung von Big Data verkomplizieren das Projekt.

Interview
mit der
Projektleitung



Herausforderung

- Notwendige Sammlung & Verarbeitung im Big Data-Umfang für effektive Bots
- Algorithmische Transparenz
- Einwilligung der Nutzer
- Modellentwicklung aus gesammelten Daten versus Recht auf Löschung. Datenminimierung bedingt möglich, da jegliche Form von Daten angegeben werden könnte.

Rechtlich

Artikel 5 (1) lit c, 6, 9, 25 DS-GVO; ePrivacy Richtlinie; BSDG, TTDSG

Technisch

Voice- & Chatbot als Servicekanal, der über einen Webkanal zugänglich ist. Analytik & KI ermöglichen automatisierte Interaktionen und einen Human Hand-over bei komplexeren Anfragen.¹

Argumentation

DZ Compliance Partner: Werden personenbezogene Daten verarbeitet, sind zahlreiche Anforderungen aus der DS-GVO zu beachten, daher u.a. Einholung der Einwilligung des Kunden, Datenschutz-Hinweise, Löschung, Verschlüsselung.⁴

Business Analyst Interviewee: Der Einsatz ist möglich, aber Chatbot-Anbieter müssen Datenschutzregularien frühzeitig im Projekt berücksichtigen und eine unternehmensweite Strategie entwickeln, mit menschlichen Agenten kombinieren, strenge Benutzerakzeptanz-Tests durchführen und Schulungen für Mitarbeitende planen.

Insider Intelligence: Verbraucherinnen und Verbraucher verlangen einen Rund-um-die-Uhr-Service in Bereichen wie Bank- und Finanzwesen, Gesundheit und Wellness.²

Anwalt C. Schwaiger: in Österreich gilt: „Für die Bürger sichtbar sind unsere Chatbots Fred im Finanzamt, Mona im Unternehmerservice-Portal und Justitia im Justizministerium.“³

Fazit

- Kosten abhängig davon, ob es sich um einen zugekauften Chatbot von Dritten oder einer Eigenentwicklung handelt bzw. auch von der regelmäßigen Wartung des Chatbots
- Das Projekt verzögert sich aufgrund der zusätzlichen Tests von DS-GVO-Szenarien a priori der Markteinführung
- Datenschutzgesetze in Europ werden strikt ausgelegt, viele Einschränkungen⁶



1 Accenture, the chatbot business & Accenture, Chatbot Credentials | 2 Insider Intelligence, Chatbot market in 2021 | 3 Kleine Zeitung, Analyse Künstliche Intelligenz | 4 DZ CompliancePartner, Ausgabe 1/2021, 14 | 5 Universität Basel, Einsatz künstlicher Intelligenz | 6 Justus-Liebig-Universität Hiessen; Chancen und Herausforderungen von Big Data, S 20 ff

Quellen Screenshots: Google Cloud Blog, MTS, Startup AI company sets out to Transform chat and Voicebot

Produktion und Energie

17%
der deutschen
Bevölkerung
hat Smart Meter
installiert⁴

53.341.369€
Gesamtsumme der
Geldbußen im Transport-
& Energiesektor⁵

43
Gesamtanzahl der
Geldbußen im Transport-
& Energiesektor⁵



Energieversorgungsunternehmen nehmen als kritische Infrastruktur eine wichtige gesellschaftliche Rolle ein. Datenschutzrechtliche Regelungen schränken Unternehmen bei Auswertung von Big Data sowie Nutzung cloudbasierter Anwendungen ein.

Herausforderungen

- Fokus von Produktionsunternehmen liegt auf Prozessen der Wertschöpfungskette, kein People-Business¹
- Risikomanagement von Cloud-Lösungen in Produktionsbranche noch unzureichend²
- Die Energiebranche zählt zur kritischen Infrastruktur und unterliegt besonderen lokalen und europäischen Regularien
- Verarbeitung besonders sensibler personenbezogener Daten wie Stromverbrauch, Name und Adresse³

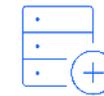
Highlights

- Schrems II Cookie-Speicherung ohne zusätzliche Schutzmaßnahmen
- Eingeschränkte notwendige Zugriffsmöglichkeiten wegen DS-GVO
- Ordnungsgemäßen Umgang mit Energieverbrauchsdaten sicherstellen
- DS-GVO-Bußgeld wegen fehlender Transparenz bei Überprüfung von Kunden-Verhaltensmustern

Anwendungsfälle



US-Cookietransfer



Datenmigration



Smart Meters



Kundenverhalten



Anwendungsfall

US-Cookietransfer

Deutsches Verwaltungsgericht Wiesbaden verbietet staatlicher Hochschule RheinMain auf deren Website www.hs-rm.de den Einsatz des Dienstes Cookiebot wegen Speicherung von Cookies bei amerikanischen Cloud-Anbietern.

Herausforderung

- Mit dem dänischen Cookiebot-Anbieter Cybot können Websitebetreiber die Einwilligung zur Speicherung von Cookies ersuchen
- Verarbeiter hatten nicht notwendigen Maßnahmen nach Schrems II ergriffen
- Datenübertragung von Websitennutzenden zu US-Servern nur mit besonderer vorheriger Absicherung¹

Rechtlich

VG Wiesbaden 01.12.2021 – 6 L 738/21.WI; DS-GVO; C-311/18 (Schrems II)

Technisch

Mit Cookiebannern können Websitennutzende um Einwilligung in die Speicherung von Cookies auf ihrem Endgerät gebeten werden.¹

Argumentation

Verwaltungsgericht Wiesbaden: Da sich Akamais Zentrale in den USA befindet, führe der Cookiebot zu einer nach der DS-GVO und Schrems II unzulässigen Übermittlung. Akamai unterliege dem Cloud Act, der US-Anbieter dazu verpflichtet, „sämtliche Daten offenzulegen, unabhängig vom Speicherort“.²

Rechtsanwalt Jonas Breyer: „spektakuläre Entscheidung“, da ein unzulässiger Datentransfer auch bei cloud-hosted Websites-Plugins vorläge. Betroffene seien u.a. reCAPTCHA und Google Analytics.¹

Angeklagte Hochschule RheinMain: Standardvertragsklauseln liegen vor. Cybot werde nur „anonymisierte“ Internetkennung, Datum und Uhrzeit der Zustimmung, Nutzeragent des Browsers, URL, anonyme, zufällige & verschlüsselte Schlüssel und Einwilligungsstatus übermittelt¹

Hessischer Datenschutzbeauftragter: Bestätigt die Verarbeitung von Klardaten mit bloßer Transportverschlüsselung und damit, dass keine ausreichenden Schutzmaßnahmen vorliegen.¹

Fazit

- Cookiebot-ähnliche Dienste (in Unternehmen, Projekten, und Apps) können Daten nur bei erheblichen Zusatzaufwand DS-GVO-konform in die USA übertragen.
- Betroffen sind Consent Management-Plattformen und Anbieter von Cookiebannern wie auch Usercentrics, SourcePoint, OneTrust, Didomi, CookieFirst, und Unternehmen, die amerikanische Cloud-Dienste nutzen. Auch betroffen sind technische Prozesse von reCAPTCHA.



¹ Heise online, Gericht: Deutsche Webseiten dürfen keine US-Cookies setzen; (2) VG Wiesbaden 01.12.2021 - 6 L 738/21.WI

Quelle Screenshots: Heise online, Gericht: Deutsche Webseiten dürfen keine US-Cookies setzen; Dr. DS-GVO, Nutzung von Cookiebot; Cookiebot; Online-Tracking

Anwendungsfall

Datenmigration

Das Projekt musste gestoppt werden, weil externen IT-Ingenieuren der Zugriff auf die zu migrierenden Daten untersagt wurde. Der Grund waren fehlende Datenklassifizierung und der Aufwand, personenbezogene und auch sensible Daten basierend auf DS-GVO-Anforderungen zu trennen und schützen.



Herausforderung

- Datenmigration von einer alten On-Premise Infrastruktur zu einer neuen Infrastruktur bzw. in die Cloud
- Externe Beraterinnen und Berater benötigen Zugriff für eine erfolgreiche Migration. Das war nicht möglich, da personenbezogene Daten a priori getrennt und geschützt werden mussten

Rechtlich

Artikel 5, 32 DS-GVO Datenminimierung; Need-to-know Principle

Technisch

Ohne angemessenen Zugriff war es nicht möglich, die Daten durch die externe Beratung ordnungsgemäß in die neue Umgebung zu migrieren.

Argumentation

Interviewee Projektleitung: Unserem Beratungsteam wurde beim Start des Projekts der Zugriff verwehrt. Personenbezogene Daten verlassen hier nicht das Unternehmen, aber der Zugriff von extern ist erschwert. Zusätzliche Maßnahmen zum Zugriff- und Consent Management erhöhen die Komplexität.

Sewobe: Fehler passierend schnell und können riesige Schäden wie z.B. verlorene personenbezogene Daten anrichten.¹

Talend: Bei der Erstellung des Datenmigrationskonzepts sollte Kenntnis über Daten vorliegen.²

Netzwoche: Nachrüsten ist teuer und aufwendig – SAP S/4Hana-Migrationen sind kostspielig bei mangelnder Qualität der Stammdaten auf Alt-Systemen.³

Fazit

- Erhöhung des Projektbudgets und -zeit durch die Einbeziehung von Spezialistinnen und Spezialisten und zusätzlicher Technologie
- Besonderer Fokus auf Qualität und Genauigkeit⁴
- Die DS-GVO bewirkt eine Umstellung von Datenmanagement, Datenschutzkonzepten und zusätzlichen organisatorischen und technische Maßnahmen auch dann, wenn Anwendungsfälle dies nicht erfordern



1 Sewobe, Leitfaden – Datenmigration leicht gemacht, 2 | 2 talend, Datemigration verstehen: Strategie und Best Practices | 3 Netzwoche, SAP/4Hana – Migration: kosten schlechter stammdaten vermeiden | 4 Accenture, Confidence in HR Conversions and Integrations, 3

Anwendungsfall

Smart Metering Systeme

Smart Metering für fortschrittliche und intelligente Messgeräte zur Erfassung von Energieverbrauchsdaten in großem Umfang und Verarbeitung in Echtzeit kreiert Bedenken um den Schutz dieser personenbezogenen Daten.

Marktforschung



Herausforderung

- Smart Metering erfasst in Echtzeit den Umfang des Energieverbrauchs
- Dies bildet personenbezogene Daten ab. Bedenken umfassen Profiling, mangelnde Kontrolle, typische Risiken von IoT-Geräten sowie potenzielle Massenüberwachung

Rechtlich

Artikel 5-6, 13-14, 15-21, 32 DS-GVO; dt. Messstellenbetriebsgesetz (MsbG); EDPS Opinion on smart metering systems; DSFA Vorlage der Europäische Kommission; Verordnung (EU) 2017/2195

Technisch

Smart Meter und intelligente Stromzähler messen den Energieverbrauch und stellen diesen Verbrauchswert täglich dem Netzbetreiber über eine Kommunikationsanbindung zu Verfügung.

Argumentation

Minister in Schleswig-Holstein: Wir brauchen das Management eines Netzes, das mit 100% Erneuerbaren läuft, intelligent speichert, verteilt und umleitet.

Energiewende-Index: 17% der dt. Bevölkerung hat Smart Meter installiert. Im Vergleich haben Skandinavien, Italien, und Spanien 97% erreicht.

Minister in Brandenburg: Bundespolitik sollte die nötigen Rahmenbedingungen für Energiewenden schaffen. Das Genehmigungsverfahren sei eine Katastrophe. Beispielsweise dauert die Übertragungsnetzleitung Uckermark bereits 16 Jahre. Beim Breitbandausbau sieht es ähnlich aus.¹

Urteil des nordrhein-westfälischen OVG: Smart Metering darf nicht eingesetzt werden.²

Generaldirektor von Edyna – größter Stromverteiler Südtirols: Smart Meter ist eine wichtige Innovation, die unser Stromnetz noch intelligenter und digitaler macht. Dadurch können wir die Energieverteilung effizienter steuern und Servicequalität verbessern. Edyna will bis 2024 Stromzähler durch Smart Meter ersetzen.³

Fazit

- Smart Metering-Anbieter haben umfassende Regelungen aus dem Energiesektor sowie Datenschutzerfordernungen nach DS-GVO (wie Rechtmäßigkeit der Verarbeitung von Energieverbrauchsdaten mit Einwilligung oder soweit gesetzlich erlaubt) einzuhalten



¹ Heise Online, Energiewende | ² Heise Online, Smart Meter | ³ Rainews, Neue Stromzähler kommen

Quelle Screenshots: [Umfrage: Interesse an "Smart Metern," in Deutschland steigt](#); [Was für ein Paukenschlag! News-Blog der datenschutz nord Gruppe](#)



Anwendungsfall

Kundenverhalten

Deutsches Energieunternehmen muss DS-GVO-Bußgeld zahlen, da gegenüber Kundinnen und Kunden die notwendige Durchsicht und Transparenz über routinemäßige Überprüfungen deren Verhaltens nicht offengelegt und darüber informiert wurde.

Herausforderung

- Das deutsche Energie-Unternehmen Vattenfall prüft routinemäßig „wechselauffälliges Kundenverhalten“
- Bei Bonus-Verträgen prüft das Unternehmen Rechnungen aus vergangenen Vertragsbeziehungen
- Betroffenen (über 500.000) war nicht erkennbar, dass ein solcher Datenabgleich stattfand

Rechtlich

Artikel 12-13 DS-GVO Transparenzgebot

Argumentation

Vattenfall: Die erfolgte Datenverarbeitung und der Abgleich seien prinzipiell rechtmäßig gewesen. Dies habe die Aufsicht „nunmehr final bestätigt“. Mit dieser „verbindlichen Klärung“ sei für Vattenfall „ein wichtiges Ziel erreicht.“¹

Hamburgische Datenschutzbehörde: Strafe wegen mangelnder Aufklärung der betroffenen Kunden. Die Strafe sollte allen Unternehmen eine Warnung sein.²

Auskunftei Schufa und Wirtschaftsauskunftei Crif Bürgel: Plan aus 2020 über Daten von Strom- und Gaskunden branchenweit zusammenzuführen, um sog. Bonushopper zu identifizieren.¹

Verbraucherzentrale Brandenburg: „Das Sammeln und Auswerten von Daten vertragstreuer Kundinnen und Kunden entbehrt jeglicher Rechtfertigung.“

Datenschutzexperte Thilo Weichert: Kunden werden so zu „Freiwild“.

Verbraucherzentrale Bundesbank (VZBV): „So ein Branchenpool könnte es Energieversorgern erleichtern, wechselwillige Kunden zu identifizieren und Vielwechsler systematisch abzulehnen.“³

Fazit

- Vattenfall hat die Strafe für die fehlende Transparenz für den Datenabgleich bekommen, und nicht für die Zulässigkeit eines solchen Abgleichs, welches noch einen Graubereich der DS-GVO darstellt
- Für Unternehmen ist der Umfang der Transparenzpflicht nach DS-GVO unklar
- Folglich akzeptiert das Unternehmen die Sanktion und erweitert gemeinsam mit der Behörde die „notwendigen Angaben“



1 Heise Online, DS-GVO: Vattenfall muss 900.000 Euro nach Bonushopper-Auslese zahlen | 2 Datenschutz-Hamburg, Bußgeld gegen Vattenfall | 3 Süddeutsche Zeitung, so sortierte Vattenfall Bonushopper aus | Quelle Screenshots: Europe.eu, Hamburg DPA; Datenschutz-Hamburg, Bußgeld gegen Vattenfall

Gesundheit

1,8 Millionen

Downloads der
CovPass App in
Deutschland²

12.510.933€

Gesamtsumme der
Geldbußen in der
Gesundheitsbranche³

79

Gesamtzahl der
verhängten Geldbußen
in der Gesundheit³



DS-GVO stellt Barrieren bei der Verbesserung und Erweiterung von Services auf, insbesondere bei der Anwendung neuer Technologien, wie AI und Cloud Services. Grund ist, dass die Komplexität Innovationen lähmt. Im Gesundheitsbereich besteht stetig die Sorge um die Sicherheit der Daten und Missbrauch durch Online-Tools.¹

Herausforderungen

- Sensible Gesundheitsdaten werden in kommerziellen Apps verwendet und interpretiert
- Datensammlungen sind nicht konform mit der DS-GVO
- Einholen von Einwilligungen im Fall von Gesundheitsvorfällen schwierig
- Funktionseinschränkungen von Gesundheits-Apps aufgrund von DS-GVO-Anforderungen
- Statusabfragen sind durch den Arbeitgeber beschränkt möglich

Highlights

- Unterschiedliche Corona-Apps in verschiedenen Ländern und Regionen, mitunter mit niedriger Anerkennung
- Einschränkungen von Gesundheitsservices
- Rechtsunsicherheit bei Anwendbarkeit

Anwendungsfälle



Corona-Apps



Fitness-Apps



**Impfabfrage durch
den Arbeitgeber**



TraumaRegister DGU®

Anwendungsfall

Corona: Kontaktverfolgungs-Apps

Digitale automatisierte Kontaktverfolgung durch Mobile Contact Tracing-Applikation am Smartphone. Beispiele sind die Stopp-Corona App vom Deutschen Roten Kreuz, Novid20¹ und die Corona-Warn-App.

Interview
mit Sales



Herausforderung

- Digitale automatisierte Kontaktverfolgung via App
- Entwicklung in wenigen Wochen
- Verarbeitung sensibler Gesundheitsdaten

Rechtlich

Artikel 6, 9, 25 DS-GVO privacy by design; DSGVO,
Artikel 7 & 8 EU-Grundrechtscharta; Artikel 8 EMRK²

Technisch

Entwicklung mittels Kontakterkennung über ein automatisches Pairing per Bluetooth, welches die betroffenen Personen anonymisiert benachrichtigt⁶

Argumentation

Deutsches Rotes Kreuz: Zur Nutzung der App müssen keine personenbezogenen Daten angegeben werden. Die Kontakte werden lediglich am Endgerät gespeichert. Bei einer Erkrankung bekommen alle in der Kontaktkette eine anonymisierte Meldung. Auch eine DSFA wurde erfolgreich vorab durchgeführt.³

Rechtsgutachten zum Einsatz von Tracing-Apps: Einwilligung als Rechtsgrundlage setzt Freiwilligkeit voraus, welches wegen der Belastungssituation, Staatsnähe, Einschränkungen der Handlungsfähigkeit ohne Installation, oder durch den Arbeitgeber oder Anbieter der Grundversorgung voraussetzt. Es braucht eine gesetzliche Absicherung der Freiwilligkeit der Einwilligung.¹

Bundesfinanzministerium: Bis zu 69 Millionen Euro kostet die Corona-Warn-App voraussichtlich.⁴

Europäisches Parlament: Corona-Apps sollten sorgfältig konzipiert sein, da sie sonst sensible Nutzerdaten offenlegen könnten. Laut Kommission soll auf Bluetooth statt auf Geolokalisierung gesetzt werden.⁵

Fazit

- Entwicklung der Applikationen binnen weniger Wochen,
- Organisationen mussten bei App-Entwicklung in kurzer Zeit die DS-GVO-Anforderungen korrekt interpretieren und implementieren, um keine Strafe zu riskieren
- Die unklaren Umsetzungsansichten erschweren DS-GVO-Konformität und verlängern Prozess der App-Entwicklung



1 Nikolaus Fargó, 28 | 2 Nikolaus Fargó, 24 | 3 StoppCorona, FAQ | 4 Der Tagesspiegel, Warum die Corona-Warn-App | 5 Europäisches Parlament, Corona-Tracing-Apps;

6 Accenture, Stopp Corona AppA | Quelle Screenshots: StoppCorona, FAQ; Accenture, Stopp Corona-App



Anwendungsfall

Corona-App: Luca

Neben den „normalen“ Kontaktverfolgungsfeatures und Risikokontaktbenachrichtigungen mit kritisch gesehenem Geofencing, hat die Luca-App auch einen wirtschaftlichen Nutzen.

Herausforderung

- Digitale automatisierte Kontaktverfolgung via App mit wirtschaftlichem Nutzen (!) wie Gästeregistrierung, Kontakttagebuch, Kontaktnachverfolgung mit Anbindung an Gesundheitsämter¹
- Verarbeitung personenbezogener Daten und sensibler Gesundheitsdaten

Rechtlich

Artikel 6, 9, 25 DS-GVO

Technisch

Entwicklung einer Kontakterkennung über ein automatisches Pairing. Luca erstellt einen persönlichen, sich ständig ändernden und verschlüsselten QR-Code⁶

Argumentation

Verbraucherzentrale: Die Luca-App sammelt im Gegensatz zur Corona-Warn-App personenbezogene Daten bei aktiver Nutzung wie den Aufenthaltsort, um Gesundheitsämter bei Bedarf zu kontaktieren. Die Corona-Warn-App appelliert an Selbstquarantäne.²

Betreiber der Luca-App: Orte werden längstens 30 Tage lang gespeichert.²

Chaos Computer Club: Behauptung von handwerklichen Mängeln und Schwachstellen.³

Kritik von 70 IT-Sicherheitsforschenden: Luca-App erfüllt nicht dieselben Prinzipien wie die Corona-Warn-App, da es u.a. keine technische Zweckbindung gibt, sondern eine private Gewinnabsicht zu erkennen ist und aufgrund des Designs ein Missbrauchsrisiko besteht.⁴

Bayerisches Staatsministerium für Digitales: Entscheidung für die Luca-App, weil hiermit die besten Voraussetzungen vorliegen, um Infektionskette konsequent zu unterbrechen.⁵

Fazit

- Es besteht viel Kritik um die Luca-App
- Im Gegensatz zur Corona-Warn-App hat die Luca-App mehr Features und ist durch die Nutzung von Geofencing genauer
- Aufgrund der verschiedenen umstrittenen Ansichten wird es den Betroffenen erschwert, innovative Projekte zu umzusetzen





Anwendungsfall

TraumaRegister DGU®

Health Research ist gehemmt! DGU sieht übertriebenen Datenschutz als Gefährdung von Menschenleben in der Schwerverletztenversorgung an.

Herausforderung

- Das TraumaRegister DGU® ist Teil der nationalen Qualitätssicherung und Versorgungsforschung
- Die zentrale Datenbank weist weniger Behandlungsverläufe auf (in 2019: -17%)
- Der DGU sieht erhebliche formale und inhaltliche Unsicherheiten bei Einholung der Einwilligungserklärung schwerverletzter Patientinnen und Patienten¹

Rechtlich

Artikel 6 und 9 DS-GVO Einwilligung

Technisch

Das TraumaRegister DGU® ist eine zentrale Datenbank, die über 450.000 Behandlungsverläufe dokumentiert. Teilnehmende Kliniken sind primär aus Deutschland, zunehmend auch aus weiteren Ländern.²

Argumentation

DGU: DS-GVO erschwert bzw. macht Qualitätssicherung und Registerforschung zunehmend unmöglich. Herausforderung ist, pseudonymisierte Daten rechtssicher zu verwenden.

DGU-Präsident: „Aber übertriebener Datenschutz macht unser seit fast 30 Jahren bestehendes TraumaRegister nun zunichte und gefährdet damit Menschenleben“.¹

Grünen-Politiker Jan Philipp Albrecht: „Das ist kompletter Unfug, um es klar zu sagen: Der EU-Gesetzgeber hat in der DS-GVO ausdrücklich geregelt, dass es in Fällen von Bewusstlosigkeit oder anderen Notfällen im Interesse des Betroffenen keiner Einwilligung bedarf.“³

Bundesdatenschutzbeauftragten Ulrich Kelber: „Natürlich darf die Datenverarbeitung in solchen geschilderten Notlagen stattfinden.“ Er habe diese Frage bereits „tausendmal geklärt“.⁴

Fazit

- Unzulängliche Interpretation der DS-GVO, die ausdrücklich die Ausnahme des öffentlichen Interesses vom allgemeinen Datenverarbeitungsverbot vorsieht⁵
- Der Fall zeigt Unsicherheit und Spielraum für Missinterpretation der DS-GVO bzw. das Unverständnis für Fehlinterpretationen





Anwendungsfall

Impfstatusabfrage

DS-GVO verlangt eine rechtliche Grundlage von Arbeitgebern, um den Impfstatus der Arbeitnehmenden obligatorisch zu erfassen. Eine solche gesetzliche Grundlage gibt es im Arbeits- und Sozialrecht aber nicht.

Herausforderung

- Frage um die Impfstatusabfrage der Arbeitnehmenden durch den Arbeitgeber
- Informationen über den Impfstatus sind ebenso Gesundheitsdaten wie das Corona-Testergebnis oder der Nachweis einer überstandenen Infektion
- Diese Informationen stehen unter besonders strengem Schutz der DS-GVO²

Rechtlich

Artikel 4 Nummer 15 DS-GVO; Artikel 9 Absatz 1 und 2 DS-GVO; § 23 IfSG

Argumentation

Bundesministerium für Gesundheit: Die Auskunftspflicht gilt nur für die genannten Einrichtungen und Unternehmen wie Heime, Schulen, und Justizvollzugsanstalten. Für die Abfrage durch den Arbeitgeber findet die DS-GVO & BDSG Anwendung.¹

DS-GVO Artikel 9 Absatz 1: „Die Verarbeitung [von] Gesundheitsdaten [...] einer natürlichen Person ist untersagt.“ Ausnahmen finden sich in Absatz 2, aufgeführt werden hier Gründe des öffentlichen Interesses im Bereich der öffentlichen Gesundheit.

Datenschutzkonferenz: In Ermangelung einer gesetzlichen Grundlage bedarf es in der Regel einer Einwilligung der Arbeitnehmenden in die Erhebung und Verarbeitung, wobei vor allem im Beschäftigungsbereich die Freiwilligkeit der Einwilligung regelmäßig problematisch ist.²

Fazit

- Die Frage um die Abfrage des Impfstatus durch den Arbeitgeber muss einzelfallabhängig geprüft werden
- Das lässt sich durch Rechtsklarheit und eine einheitliche Lösung erreichen. Beide Voraussetzungen sind aktuell nicht gegeben²



(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.



Anwendungsfall

Mobile Health Apps

Auf Smartphones können weder automatische Messungen durch mobile Health Apps deaktiviert, noch die Applikationen endgültig vom Gerät deinstalliert werden. Was ist erlaubt und was nicht?

Herausforderung

- Datenschutzbedenken bei gesundheitsbezogenen Apps wie Apple Health (iOS) und Google Fit (Android)
- Apps sammeln sensible Daten von Nutzenden, meist automatisch
- Apps lassen sich nicht vom Endgerät deinstallieren
- Unklar ist der Datenaustausch mit anderen Apps untereinander¹

Rechtlich

Artikel 5, 6, und 17 DS-GVO; C-311/18 (Schrems II)

Technisch

Vorinstallierte Apps auf Smartphones, die Daten sammeln. Bei Google Fit werden die Daten zudem in einem zentralen Respository in der Cloud gespeichert.²

Argumentation

Studie zur Problematik von mobilen Health Apps: Google bietet einen Großteil seiner Produkte kostenlos an und speichert Daten wie Rechnungen, Dokumente, Gesundheitsdaten oder Videos. Gleichzeitig ist Google eine der größten Werbeplattformen.³

Aspekte zu Apple Health: Daten werden lokal gespeichert und verschlüsselt. Nutzende können weder die Messungen abschalten, noch ist der Datenaustausch transparent.²

Aspekte zu Google Fit: Es existieren keine besonderen Schutzvorkehrungen, dafür gibt es kommerzielle Kooperationen und automatische Messungen.²

Fortune Business Insights: Die COVID-19-Pandemie führte 2020 zu einem Download-Zuwachs für mobile Health Apps von 66%.⁴

Europäische Kommission: Ein Verhaltenskodex soll das Vertrauen der Nutzenden fördern und einen Wettbewerbsvorteil verschaffen.⁵

BVDW: Faktencheck und Antworten auf Mythen und Halbwahrheiten zu digitaler Gesundheit.

Fazit

- Der Umgang mit Gesundheitsdaten, die durch mobile Apps gesammelt und auch zwischen Apps übertragen werden, ist für die Nutzenden oft nicht transparent
- Nutzende können nicht selbst über die Messung durch ihr Smartphone entscheiden
- DS-GVO lässt mehrere Öffnungsklauseln für den öffentlichen Sektor und das Gesundheitswesen¹



¹ Sulejman Ganibegovic, 4 | ² Sulejman Ganibegovic, 12-15 | ³ Sulejman Ganibegovic, 52-53 | ⁴ Fortune Business Insights, Report ID: FBI102020 | ⁵ EC, Privacy code of conduct on mobile health apps | ⁶ BVDW, Mobile Health im Faktencheck

Quelle Screenshot: [IKU, Datenschutzrechtliche Problematik von mHealth-Apps und Wearables.docx](#)

Telekommunikation

2. Platz
der Anzahl
verhängter
Geldbußen¹

369.724.441€
Gesamtsumme
verhängter
Geldbußen¹

159
Gesamtanzahl
verhängter
Geldbußen¹



Bei einem Anteil personenbezogener Daten von fast 90% des gesamten Traffics existiert bei Telekommunikationsanbietern ein hohes Bewusstsein für Datenschutz, Vertrauen, und Datensicherheit. Die Herausforderung besteht darin, rechtliche Vorschriften in technische und betriebliche Lösungskonzepte zu übersetzen, die in technische Lösungen implementiert werden können. Bis zu 40% mehr Aufwand für Datenschutzthemen im Vergleich zur Zeit vor der Einführung der DS-GVO.

Herausforderungen

- Stark reglementierter Geschäftsbereich (TKT, DS-GVO, ITSG)
- Das Geschäftsmodell baut auf Kommunikationsangeboten auf
- Sammeln viele persönliche Daten wie zu Navigation, Wohnorte, Anruflisten
- Internationale Zusammenarbeit durch interne und externe Kooperationen wie der Abschluss von AVV, Datenübertragung
- Rechtsunsicherheit trotz behördlichem Review. Datenschutzbeauftragte suchen Klarheit, um Grauzonen der DS-GVO zu meiden

Highlights

- Schrems II verhindert die Umsetzung von Digitalisierungsprojekten wie die Entwicklung neuer Anwendungen, insbesondere bei Nutzung von DevOps und Einbeziehung grenzüberschreitender Teams
- Stringenter Dokumentations- und Schulungsaufwand
- Erhebliche Kostenfolgen bei der Inanspruchnahme von Diensten Dritter

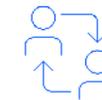
Anwendungsfälle



**App-Entwicklung
außerhalb der EU**



**Bereitstellung von
Dienstleistungen**



**Auslagerung von
Dienstleistungen an Dritte**



Anwendungsfall

App-Entwicklung- und Verbesserung

DS-GVO-Anforderungen begrenzen die Analyse personenbezogener Daten für die Effizienzsteigerungen von Big Data-Analysen. Dadurch entstehen Wettbewerbsnachteile und hohe Kosten. Qualitätspotenziale der entwickelten Anwendungen werden nicht ausgeschöpft.

Herausforderung

- Entwicklung und Verbesserung von Apps
- Schwierige Auswertung personenbezogener Daten in Big Data-Analysen maskieren
- Neue Funktionalitäten für über 400 IT-Applikationen können nur eingeschränkt weiterentwickelt werden

Rechtlich

DS-GVO; C-311/18 (Schrems II); Schwedischer Data Protection Act (2018:218) & Data Protection Ordinance (2018:19)

Technisch

Entwicklung und Verbesserung von Softwareanwendungen ohne aktuelle Daten war herausfordernd und basierte auf nicht standardisierten Verfahren.

Argumentation

Projektteam: Das Aufbereiten und die Analyse von Verarbeitungsdaten ermöglichen eine enorme Effizienzsteigerung und Strukturierung bestehender Abwicklungsprozesse. Dadurch können signifikante Einsparungen und kürzere Bearbeitungsprozesse ermöglicht werden

Die verwendeten Daten werden dazu in sogenannten Data Lakes zusammengefasst und ausgewertet.

Aufgrund der Einschränkungen durch die DS-GVO ist die Erstellung von Data Lakes nur begrenzt oder mit massiven Einschränkungen möglich.

Dies reduziert die Qualität der Ergebnisse und führt zusätzlich zu Wettbewerbsnachteilen.

Fazit

- Ressourcen in Europa sind kostspieliger als bspw. in Indien
- Die Markteinführungszeit der App hat sich aufgrund der großen Datenmengen erhöht
- Wettbewerbsverzerrungen und Einschränkung von Globalisierungsmöglichkeiten
- Anstelle globaler Lösungen, Bereitstellung lokaler Dienste für verschiedene Länder
- Große Rechtsunsicherheit über Notwendigkeit und Eignung von Maßnahmen
- Übermittlung ins Ausland ist nicht möglich und verhindert so die Qualitätssicherung dieser Daten. Adoptionen sind kostenintensiv

06

Limitationen und Bibliographie

Limitationen der Studie

Ausgangssituation

Wie bei jedem Forschungsprojekt handelt es sich bei der vorliegenden Studie um eine Momentaufnahme der derzeitigen Situation. Die abgebildeten Anwendungsfälle und Branchen sind eine reine Selektion vieler weiterer Anwendungsfälle und Branchen. Die Beschreibung und Recherche zu den Anwendungsfällen sind geprägt von Aktualität, persönlichem Input der Interviewees und somit auch mit Unsicherheiten und Unwägbarkeiten behaftet. Die Autorenschaft ist sich voll und ganz bewusst, dass der entwickelte Content verschiedene selektierte Anwendungsfälle und Branchen darstellen soll, mit Potenzial für weitere Studien zum Deep-Dive. Dennoch stellt die Studie eine umfangreiche Abbildung verschiedener Anwendungsfälle aus unterschiedlichen Branchen dar und zeigt mit den zugrundeliegenden Annahmen in eine klare Richtung: Datenschutzbedenken spielen eine signifikante Rolle.

Limitationen der Studie

Limitationen umfassen unter anderem:

- Der geografische Umfang der Studie umfasst Europa mit dem Fokus auf Deutschland. Die Anwendungsfälle und Branchen-Erklärungen beziehen sich hauptsächlich auf europäische Unternehmen und Regularien, wobei nicht ausgeschlossen werden kann, dass sporadisch auch auf außereuropäische Studien, Fachzeitschriften und anderen Materialien zurückgegriffen wird.
- Der Zeitraum der Inputdaten für die Studie umfasst 2016 bis 2022, wobei wenn möglich die neusten Materialien herangezogen werden und nicht auszuschließen ist, dass auch ältere Daten als der erwähnte Zeitraum verwendet wurden.
- Die Interviewees sind Personen aus der täglichen Unternehmenspraxis, die für die Studie ihr persönliche Einschätzung mitteilen. Dafür wird keine Richtigkeitsgarantie übernommen.
- Die Erhebung der Primärdaten erfolgt durch den Interviewer in der möglichst neutral und objektiv.
- Die Studie stellt eine Momentaufnahme dar und identifiziert Beispiele, in denen datenschutzrechtliche Herausforderungen im individuellen Innovations- und Digitalisierungsprozess erkennbar sind.
- Die Begriffe „Digitalisierung“ und „Innovation“ werden gleichbedeutend behandelt. Im Rahmen der Studie umfasst Digitalisierung den vernetzten Einsatz von Informations- und Kommunikationstechnologien zur Automatisierung betrieblicher Prozesse sowie der Entwicklung neuer Produkte und Dienste. Ziel ist die Steigerung der Wertschöpfung.¹

Interview-Protokollierung

Alle Interviews wurden manuell protokolliert, Frage und Antwort jeweils in ein gesammeltes Dokument eingepflegt.

General Questions									
Question	Answer	Question	Answer	Question	Answer	Question	Answer	Question	Answer
What is your role in the project?	...	What kind of barriers can you identify with your projects?	...	What was the company size, industry, project scope & location?	...	How did you overcome that barrier? What was the solution strategy? (e.g., get a specialist on DP)	...		
...

<p>Breakdown your Role</p> <p>Since Feb 2021 with acn - Bank, insurance companies, digitalization projects (data warehousing, ...) - Banking and finance background</p>	<p>What kind of barriers can you identify with your projects?</p> <p>data privacy as a barrier as such for banking client since they are very concerned about disclosure of data since they process very sensitive client data</p> <p>e.g., much more hesitant to move into AWS cloud since this constitutes a data transfers to a third party</p> <p>BC of this for banks is harder to make use of</p> <p>The barriers are more conceptual, identifying data and making the client aware of the importance of data is a challenge.</p>	<p>What was the company size, industry, project scope & location?</p> <p>Big European Bank 2 projects</p> <p>1] improve data warehousing / data mgmt: transfer of confidential client information from one legal entity to another</p> <p>2] chat-/voicebots: automated answering machine for questions of clients / potential clients (usually over time) over the internet, with the goal not to have to communicate to a real person</p> <p>Big German Chemical company - Big German automobile company - Manufacturing company</p>	<p>How did you overcome that barrier? What was the solution strategy? (e.g., get a specialist on DP)</p> <p>Big European Bank 2 projects</p> <p>1] Ensure data data is scrapped</p> <p>2] Agreement that data will be processed and forwarded to the bank since everyone can chat with the bot and provide any information, always a human involved, since the client information will be just forwarded to a real banker and no fully automated response</p> <p>Bringing specialist into the project to help clients identify the critical data that need to be protected.</p>
--	--	---	--

Bibliographie

Bereichsspezifische Referenzen

Allgemein

- 1 Accenture. (2021). Accenture Research Journal FY2021. <https://collections.accenture.com/collection.aspx?b=ec782f2e-4620-ec11-b12e-0a0b3d281f9d>
- 2 VG Wiesbaden. (2021). Presseinformation vom 06.12.2021: Cookie-Dienst Nr. 17/2021. <https://verwaltungsgerichtsbarkeit.hessen.de/pressemitteilungen/cookie-dienst>
- 3 EuGH, Urteil vom 16.Juli 2020 – C-311/18 [ECLI:EU:C:2020:559], Facebook Ireland und Schrems
- 4 Verordnung (EU) 2016/679 des europäischen Parlaments und des Rates vom 16. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinien 95/46/EG (ABl. L 119/1 (Datenschutz-Grundverordnung))
- 5 DSG, Bescheid vom 22. Dezember 2021 – GZ: D155.027 2021-0.586.257 (zH NOYB – European Center for Digital Rights). <https://www.dsb.gv.at/>
- 6 Accenture. (2021). Cloud Continuum: Ever-ready for every opportunity. <https://www.accenture.com/us-en/insights/cloud/cloud-continuum>
- 7 CMS. (2021). Enforcement Tracker. <https://www.enforcementtracker.com/?imprint>
- 8 Bitkom. (2021). Datenschutz als Daueraufgabe für die Wirtschaft: DS-GVO & internationale Datentransfers. <https://www.bitkom.org/sites/default/files/2021-09/bitkom-charts-pk-datenschutz-15-09-2021.pdf>
- 9 Lernende Systeme. (2020). Von Daten zu Wertschöpfung. https://www.plattform-lernende-systeme.de/files/Downloads/Publikationen/PLS_Booklet_Datenoekosysteme.pdf
- 10 BMWK. (2021). Herausforderungen beim Einsatz von Künstlicher Intelligenz. https://www.de.digital/DIGITAL/Redaktion/DE/Digitalisierungsindex/Publikationen/publikation-download-ki-herausforderungen.pdf?__blob=publicationFile&v=3
- 11 Bitkom. (2016). Digitale Prozesse. Begriffsabgrenzung und thematische Einordnung. <https://www.bitkom.org/sites/default/files/file/import/160803-Whitepaper-Digitale-Prozesse.pdf>

Bibliographie

Fachspezifische Referenzen

Mobilität

- 1 Statista. (2021). Autonomous vehicle readiness index APAC 2020, by country or region. Statista Research Department. <https://www.statista.com/statistics/1012679/apac-autonomous-vehicle-readiness-index/>
- 2 Bayern Innovativ. (2021). Künstliche Intelligenz für das automatisierte Fahren – Mit KI auf der Überholspur. <https://www.bayern-innovativ.de/seite/kuenstliche-intelligenz-fuer-das-automatisierte-fahren>
- 3 BMVi. (2021). Gesetz zum autonomen Fahren tritt in Kraft. <https://www.bmvi.de/SharedDocs/DE/Artikel/DG/gesetz-zum-autonomen-fahren.html>
- 4 Ibi research an der Universität Regensburg GmbH. (2021). Schlussbericht Empirie zu personalisierten Preisen im E-Commerce. https://www.bmj.de/SharedDocs/Downloads/DE/Service/Fachpublikationen/Schlussbericht_Empirie.pdf?__blob=publicationFile&v=1
- 5 Airbnb. Hilfe-Center: Intelligente Preisgestaltung. <https://www.airbnb.de/help/article/1168/intelligente-preisgestaltung>. (angerufen am 30. Jänner 2022)
- 6 Ann-Katrin Jeske. (2021). Studie zum Online-Handel Personalisierte Preise gibt es fast nie. <https://www.deutschlandfunk.de/studie-zum-online-handel-personalisierte-preise-gibt-es-100.html>
- 7 Olaf Rossow. (2021). Die Risikoanalyse nach Artikel 32 DS-GVO. DSB 07+08/2021. <https://www.datenschutz-notizen.de/wp-content/uploads/2021/09/Die-Risikoanalyse-nach-Artikel-32-DSGVO.pdf>
- 8 DSK. (2020). Das StandardDatenschutzmodell - Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele. Version 2.0b von der 99.Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 17. April 2020 beschlossen. https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode_V2.0b.pdf
- 9 Mailjet. Sicherheit & Datenschutz - Mailjet ist ISO 27001 zertifiziert und DS-GVO-konform. Wir beantworten Ihre häufig gestellten Fragen. <https://www.mailjet.de/sicherheit-datenschutz/>. (abgerufen am 31. Dezember 2021)
- 10 Finanzen.at. (2021). Daimler-Chef: Im Wettbewerb mit Tech-Giganten mit Datenschutz punkten. <https://www.finanzen.at/nachrichten/aktien/daimler-chef-im-wettbewerb-mit-tech-giganten-mit-datenschutz-punkten-1030612723>
- 11 Heycar. (2021). Ab 2022 verpflichtend – diese Assistenzsysteme solltest du kennen. <https://hey.car/magazine/ab-2022-verpflichtend-diese-assistenzsysteme-solltest-du-kennen>
- 12 Gartner. Information Technology Glossary: Telematics. <https://www.gartner.com/en/information-technology/glossary/telematics>. (abgerufen am 31. Jänner 2021)

Bibliographie

Fachspezifische Referenzen

Bildung

- 1 Silvia Lipp. (2021). Learning Analytics – Datenschutzrechtliche Bestimmungen als Ausgangspunkt einer verantwortungsvollen Nutzung von Bildungsdaten. Innsbruck University Press. 2021. 121-133. https://www.uibk.ac.at/iup/buch_pdfs/datapolitics/10.15203-99106-046-8-12.pdf
- 2 Europäisches Parlament. (2021). Bericht über künstliche Intelligenz in der Bildung, der Kultur und dem audiovisuellen Bereich im Verfahren 2020/2017(INI). https://www.europarl.europa.eu/doceo/document/A-9-2021-0127_DE.html
- 3 Computerwelt. (2021). KI-Regulierung zwischen Chancen und Risiken. <https://computerwelt.at/news/topmeldung/ki-regulierung-zwischen-chancen-und-risiken/>
- 4 Forum Bildung Digitalisierung, (2021). Datenschutz und digitale Schule. https://www.forumbd.de/app/uploads/2021/05/210520_FBD_ImpulspapierDatenschutz.pdf
- 5 GEW. (2019). Learning Analytics und Big Data in der Bildung. <https://www.gew.de/index.php?eID=dumpFile&t=f&f=91791&token=702ec8d5f9770206a4aa8a1079750ec9021b90bf&sdownload>
- 6 Bertelsmann Stiftung. (2021). KI in Unternehmen - Ein Praxisleitfaden zu rechtlichen Fragen. https://www.bertelsmann-stiftung.de/fileadmin/files/user_upload/KI_in_UN.pdf
- 7 Elena Schmeing. (2021). Akzeptanzkriterien für den Einsatz von Learning Analytics an deutschen Schulen. <http://publications.rwth-aachen.de/record/835563/files/835563.pdf>
- 8 Microsoft. (2021). Faktencheck Datenschutz: Wie wir unsere Kundendaten nach dem Schrems-II-Urteil schützen. <https://news.microsoft.com/de-de/datenschutz-wie-wir-unsere-kundendaten-nach-dem-schrems-ii-urteil-schuetzen/>
- 9 BlnBDI. (2021). Hinweise für Berliner Verantwortliche zu Anbietern von Videokonferenzdiensten. https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2021-BlnBDI-Hinweise_Berliner_Verantwortliche_zu_Anbietern_Videokonferenz-Dienste.pdf
- 10 KM-BW. (2021). Datenschutzkonforme Bildungsplattform kommt – Vorerst keine pauschale Untersagung von Microsoft-Produkten. <https://km-bw.de/,Lde/startseite/service/2021-07-22+Vorerst+keine+pauschale+Untersagung+von+Microsoft-Produkten?QUERYSTRING=microsoft>
- 11 Eric Heitzer. (2021). Rechtsgutachten „Digitalpakt Schule“. Der Digitalpakt Schule Eine datenschutzrechtliche Herausforderung. https://www.dgc-integrity.de/wp-content/uploads/Rechtsgutachten_Digitalpakt_Schule.pdf

Bibliographie

Fachspezifische Referenzen

Bildung

- 12 BayLfD. (2021). Aktuelle Kurz-Information 39: Office-Anwendungen aus Drittstaaten bei bayerischen öffentlichen Stellen. <https://www.datenschutz-bayern.de/datenschutzreform2018/aki39.html>
- 13 Ministerium NRW. Fragen und Antworten zum Datenschutz im Schulbereich. <https://www.schulministerium.nrw/fragen-und-antworten-zum-datenschutz>. (abgerufen am 31. Dezember 2021)
- 14 Süddeutsche Zeitung. (2021). Streit um Vergabe von Videosystem: Land unterliegt. <https://www.sueddeutsche.de/bildung/schulen-wiesbaden-streit-um-vergabe-von-videosystem-land-unterliegt-dpa.urn-newsml-dpa-com-20090101-211223-99-490616>
- 15 Moritz Tremmel. (2021). Nutzung von Google-Diensten an einer von 7 Schulen verboten. <https://www.golem.de/news/dortmund-nutzung-von-google-diensten-an-einer-von-7-schulen-verboten-2109-159792.html>
- 16 CHECK.point e-Learning. Bildungsplattform – debatte - Lernmanagementsysteme derzeit die bessere Lösung. <https://www.checkpoint-elearning.de/schule/lernmanagementsysteme-derzeit-die-bessere-loesung>. (abgerufen am 31. Dezember 2021)
- 17 HDBI. (2021). Videokonferenzsysteme in Schulen - Klarstellung zu MS-Teams und dem Auslaufen der Duldung. <https://datenschutz.hessen.de/datenschutz/hochschulen-schulen-und-archive/klarstellung-zu-ms-teams-und-dem-auslaufen-der-duldung>
- 18 OLG Frankfurt am Main. (2021): Presseinformation vom 23.12.2021 Nr. 82/2021: Ausschreibung von Videokonferenzsystemen für die hessischen Schulen vergabewidrig. <https://ordentliche-gerichtsbarkeit.hessen.de/pressemitteilungen/ausschreibung-von-videokonferenzsystemen-f%C3%BCr-die-hessischen-schulen-vergabewidrig>
- 19 It-daily.net. (2021). Classroom-Lösung: Teamviewer steigt in Bildungsmarkt ein. <https://www.it-daily.net/shortnews/30651-classroom-loesung-teamviewer-steigt-in-bildungsmarkt-ein>
- 20 Ewald Hetrodt. (2021). Entscheidung vom OLD Frankfurt - Neue Ausschreibung für Konferenz-Software für Schulen notwendig. <https://www.faz.net/aktuell/rhein-main/online-unterricht-soll-datenschutz-regeln-in-hessen-einhalten-17703477.html>

Bibliographie

Fachspezifische Referenzen

Finanzdienstleistungen

- 1 Mike Leone. (2021). The Path to Data Leadership: Embracing embedded analytics and a comprehensive data analytics platform. TechTarget. <https://www.intersystems.com/isc-resources/wp-content/uploads/sites/24/ESG-eBook-Embedded-Analytics-Trends.pdf>

- 2 Staperior. DS-GVO und ihre Auswirkungen auf den Bankensektor in Deutschland. <https://staperior.de/dsgvo/>. (abgerufen am 31 Dezember 2021)

- 3 Monika Prinz. (2021). Microsoft Finanzmonitor: So steht es um Digitalisierung und Nachhaltigkeit in der Finanzbranche. Microsoft Branchenblogs. <https://cloudblogs.microsoft.com/industry-blog/de-de/financial-services/2021/04/29/microsoft-finanzmonitor-so-steht-es-um-digitalisierung-und-nachhaltigkeit-in-der-finanzbranche/>

- 4 Corinna Ewelt-Knauer; Barbara E. Weißenberger; Peter Kotzian; Mohamed Amin Khaled. (2019). Chancen und Herausforderungen von Big Data im digitalisierten Geschäftsumfeld von Banken. Justus-Liebig-Universität Gießen in Zusammenarbeit mit GBB-Rating Gesellschaft für Bonitätsbeurteilung mbH. https://www.gbb-rating.eu/de/Documents/Digitalisierung_Brosch%C3%BCre%20CEK%202018%2017%2004%20MK%2010%2007%20final.pdf

- 5 Roman Vilgut. (2021). Analyse Künstliche Intelligenz: Der rechtsfreie Raum hat ein Ende. Kleine Zeitung. https://www.kleinezeitung.at/wirtschaft/5971384/Analyse_Kuenstliche-Intelligenz_Der-rechtsfreie-Raum-hat-ein-Ende

- 6 DZ CompliancePartner. (2021). Point of Compliance Ausgabe 1/2021. https://www.dz-cp.de/dateien/pdf/poc/poc_1_2021.pdf

- 7 Nadja Braun Binder; Matthias Spielkamp; Catherine Egli; Laurent Freiburghaus; Eliane Kunz; Nina Laukenmann; Michele Loi; Anna Mätzener; Liliane Obrecht; Jessica Wulf. (2021). Einsatz künstlicher Intelligenz in der Verwaltung: rechtliche und ethische Fragen. Schlussbericht vom 28. Februar 2021 zum Vorprojekt IP6.4. Universität Basel im Auftrag von Staatskanzlei Kanton Zürich. https://www.zh.ch/content/dam/zhweb/bilder-dokumente/themen/politik-staat/kanton/digitale-verwaltung-und-e-government/projekte_digitale_transformation/ki_einsatz_in_der_verwaltung_2021.pdf

- 8 Accenture. (2020). Chatbot Overview and Case Studies - October 2017. <https://kxdocuments.accenture.com/Contribution/a52f81f0-ef18-4c13-b28c-4422dd989815>

Bibliographie

Fachspezifische Referenzen

Produktion und Energie

- 1 Isap magazin. (2018). Der Fokus im produzierenden Gewerbe. <https://isap.de/magazin/detail/Blog/Post/zeige/der-fokus-im-produzierenden-gewerbe/>
- 2 Christian Jäger. (2020). Darum ist die DS-GVO in der Energiebranche so wichtig. Energie Digitalisieren. <https://energie-digitalisieren.de/knowhow/darum-ist-die-dsgvo-in-der-energiebranche-so-wichtig/>
- 3 Stefan Kreml. (2021). Energiewende: Schleswig-holsteinischer Minister fordert mehr Smart Meter. Heise Online. <https://www.heise.de/news/Energiewende-Schleswig-holsteinischer-Minister-fordert-mehr-Smart-Meter-6295202.html>
- 4 Stefan Kreml. (2021). Gericht: Deutsche Webseiten dürfen keine US-Cookies setzen. Heise Online. <https://www.heise.de/news/Gericht-Deutsche-Webseiten-duerfen-keine-US-Cookies-setzen-6288818.html>
- 5 Jan Klos. (2021). Leitfaden – Datenmigration leicht gemacht. SEWOBE. https://www.sewobe.de/fileadmin/download/sewobe/Datenmigration_Leitfaden_SEWOBE.pdf
- 6 Talend. Datenmigration verstehen: Strategie und Best Practices. <https://www.talend.com/de/resources/datenmigration-strategien-und-best-practises/>. (abgerufen am 31. Dezember 2021)
- 7 Matthias Förg. (2021). SAP S/4Hana-Migration: Kosten schlechter Stammdaten vermeiden. netzwoche. <https://www.netzwoche.ch/news/2021-06-23/sap-s4hana-migration-kosten-schlechter-stammdaten-vermeiden>
- 8 Accenture. (2020). Confidence in HR Conversions and Integrations. https://www.accenture.com/_acnmedia/PDF-105/Accenture-Confidence-HR-Conversions-Integrations.pdf#zoom=50
- 9 Stefan Kramp. (2021). Smart Meter: Gericht stoppt Einbaupflicht intelligenter Stromzähler. Heise Online. <https://www.heise.de/news/Smart-Meter-Gericht-stoppt-Einbaupflicht-intelligenter-Stromzaehler-5073655.html>
- 10 Rainews. (2021). Südtirol - Neue Stromzähler kommen. <https://www.rainews.it/tgr/tagesschau/articoli/2021/12/tag-edyna-neue-stromzaehler-smart-meter-d1da1f87-808f-424f-97d9-e824467688d7.html>
- 11 Stefan Kreml. (2021). DS-GVO: Vattenfall muss 900.000 Euro nach Bonushopper-Auslese zahlen. Heise Online. <https://www.heise.de/news/DSGVO-Vattenfall-muss-900-000-Euro-nach-Bonushopper-Auslese-zahlen-6200668.html>
- 12 HmbBfDI. (2021). Bußgeld gegen Vattenfall Europe Sales GmbH verhängt. <https://datenschutz-hamburg.de/pressemitteilungen/2021/09/2021-09-25-vattenfall2>
- 13 Nils Wischmeyer. (2021). Stromkunden - So sortierte Vattenfall Bonushopper aus. Süddeutsche Zeitung. <https://www.sueddeutsche.de/wirtschaft/vattenfall-bonushopper-bussgeld-datenschutz-1.5419904>

Bibliographie

Fachspezifische Referenzen

Gesundheit

- 1 Accenture. (2021). Der Patient im Mittelpunkt. https://www.accenture.com/_acnmedia/PDF-166/Accenture-Oesterreich-Gesundheitsstudie-Der-Patient-Im-Mittelpunkt-2021.pdf#view=50
- 2 Statista. (2021). Most downloaded Android health apps in Germany 2021. L.Ceci. <https://www.statista.com/statistics/858810/most-downloaded-health-fitness-apps-germany/>
- 3 Nikolaus Forgo. (2020). Einige Bemerkungen zu datenschutzrechtlichen Rahmenbedingungen des Einsatzes von Tracing-Apps zur Bekämpfung der COVID-19-Krise. Stellungnahme auf Anfrage von Abg. Z. Nr. Mag. Christian Drobits, SPÖ-Datenschutzsprecher am 13.04.2020. https://id.univie.ac.at/fileadmin/user_upload/i_id/Website_Header_IDLaw/Gutachten13.pdf
- 4 Österreichisches Rotes Kreuz. Fragen und Antworten zur Stopp Corona-App. https://www.stopp-corona.at/faq_stopp_corona_app/. (abgerufen am 31. Dezember 2021)
- 5 Oliver Voss. 69 Millionen Euro - Warum die Corona-Warn-App so viel kostet. Tagesspiegel. <https://www.tagesspiegel.de/wirtschaft/69-millionen-euro-warum-die-corona-warn-app-so-viel-kostet/25929302.html>
- 6 Europäisches Parlament. (2020) Corona-Tracing-Apps: Schutz der Privatsphäre, grenzüberschreitende Nutzung. <https://www.europarl.europa.eu/news/de/headlines/society/20200429STO78174/corona-tracing-apps-schutz-der-privatsphare-grenzüberschreitende-nutzung>
- 7 Accenture. (2020). Stopp Corona-App - COVID-19-Digitale Kontaktverfolgung hilft, die Kurve abzuflachen. https://www.accenture.com/_acnmedia/PDF-130/Accenture-Stopp-Corona-App-AT.pdf#zoom=40
- 8 Ihk-München und Oberbayern. Welche Rolle spielt die Luca App und wie setzt man sie ein?. IHK-Ratgeber. <https://www.ihk-muenchen.de/de/Service/Recht-und-Steuern/Arbeitsrecht/Bestehende-Arbeitsverh%C3%A4ltnisse-K%C3%BCndigung-und-Sozialversicherung/Corona-Virus-Dienstreisen-Arbeitsausfall-Arbeitsschutz/Infektionsschutz-bei-der-%C3%96ffnung-von-Unternehmen/luca-app/>. (angerufen am 31. Dezember 2021)
- 9 Verbraucherzentrale NRW. (2022). Was „luca“ anders macht als die Corona-Warn-App. <https://www.verbraucherzentrale.de/wissen/digitale-welt/apps-und-software/was-luca-anders-macht-als-die-coronawarnapp-57918>
- 10 CCC. (2021). Luca App: CCC fordert Bundesnotbremse. <https://www.ccc.de/de/updates/2021/luca-app-ccc-fordert-bundesnotbremse>
- 11 Digikoletter. (2021). Gemeinsame Stellungnahme zur digitalen Kontaktnachverfolgung. <https://digikoletter.github.io/>
- 12 Luca app. Gemeinsam das Leben erleben. <https://www.luca-app.de/>. (abgerufen am 31. Dezember 2021)

Bibliographie

Fachspezifische Referenzen

Gesundheit

- 13 Stmd Bayern. Kontaktnachverfolgungs-App - Bayern setzt auf luca App zur Corona-Kontaktnachverfolgung. <https://www.stmd.bayern.de/themen/kontaktnachverfolgungs-app/>. (abgerufen am 31. Dezember 2021)
- 14 DGU. (2021). DGU-Präsident: „Übertriebener Datenschutz gefährdet Menschenleben in der Schwerverletztenversorgung“. Pressemitteilung der DGU. [www.dgu-online.de /presse/pressemitteilungen/detailansicht-pressemitteilungen/artikel/dgu-praesident-uebertriebener-datenschutz-gefaehrdet-menschenleben-in-der-schwerverletztenversorgung-2-2252](http://www.dgu-online.de/presse/pressemitteilungen/detailansicht-pressemitteilungen/artikel/dgu-praesident-uebertriebener-datenschutz-gefaehrdet-menschenleben-in-der-schwerverletztenversorgung-2-2252)
- 15 AUC. TraumRegister DGU®. <https://www.traumaregister-dgu.de/>. (abgerufen am 31. Dezember)
- 16 Twitter. Tweet von Jan Philipp Albrecht am 28. Oktober 2021 07:11 am. <https://twitter.com/JanAlbrecht/status/1453590228585885700>. (abgerufen am 31. Dezember 2021)
- 17 Twitter. Tweet von Alricht Kelber am 28. Oktober 2021 09:32 am. <https://twitter.com/UlrichKelber/status/1453625828986826756>. (abgerufen am 31. Dezember 2021)
- 18 Christiane Schulzki-Haddouti. (2021). DSGVO-Kritik von Unfallmediziner: Heftiger Widerspruch der Experten. Heise online. <https://www.heise.de/news/DSGVO-Kritik-von-Unfallmediziner-Heftiger-Widerspruch-der-Experten-6234406.htm>
- 19 Bundesministerium für Gesundheit. FAQ Impfstatusabfrage bei Arbeitnehmerinnen und Arbeitnehmern. <https://www.bundesgesundheitsministerium.de/coronavirus/faq-arbeitnehmerselbstaendige/faq-impfstatusabfrage.html>. (abgerufen am 31. Dezember 2021)
- 20 DSK. (2021). Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 29.03.2021. https://www.datenschutzkonferenz-online.de/media/en/20210331_entschliessung_impfdatenverarbeitung.pdf
- 21 Sulejam Ganibegovic. (2020). Datenschutzrechtliche Problematik von mHealth-Apps und Wearables im Bezug auf das europäische und österreichische Datenschutzrecht. JKU Universität Linz. <https://epub.jku.at/obvulihs/download/pdf/4917082?originalFilename=true>
- 22 Fortune Business Insights. (2021). Market Research Report 2020. Report ID: FBI102020. <https://www.fortunebusinessinsights.com/enquiry/request-sample-pdf/mhealth-apps-market-102020>.
- 23 Europäische Kommission. Privacy code of conduct on mobile health apps. <https://digital-strategy.ec.europa.eu/en/policies/privacy-mobile-health-apps>. (abgerufen am 31. Dezember 2021)
- 24 BVDW. (2016). Mobile Health im Faktencheck. https://www.bvdw.org/fileadmin/bvdw/upload/publikationen/digital-commerce/201611_ES_BVDW_Leitfaden_Mobile_Health_2016.pdf

Ihr Projektteam

Bitkom e. V.
Albrechtstraße 10
10117 Berlin

bitkom.org



Susanne Dehmel

Mitglied der Geschäftsleitung
Recht & Sicherheit
s.dehmel@bitkom.org



Rebekka Weiß

Leiterin Vertrauen & Sicherheit
T +49 (0)15117439698
r.weiss@bitkom.org

Ihr Projektteam

Accenture
Campus Kronberg 1
61476 Kronberg im Taunus

[accenture.de](https://www.accenture.de)



Raimund Wilhelmer

Principal Director Security
Innovation

raimund.wilhelmer@accenture.com



Prithwi Lahiri

Security Consulting
Consultant

prithwi.lahiri@accenture.com



Doris Winkler

Security Consulting Analyst
Accenture

doris.winkler@accenture.com

Bitkom vertritt mehr als 2.000 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player.

Bitkom e. V.
Albrechtstraße 10
10117 Berlin

T 030 27576-0
bitkom@bitkom.org

[bitkom.org](https://www.bitkom.org)

bitkom