



Datenschutz als Herausforderung für die Digitalisierung

Studie zur Erhebung von Anwendungsfällen in Europa mit
Schwerpunkt Deutschland

Juni 2022

Eine gemeinsame Studie von

 **accenture**

bitkom

Agenda

Datenschutz als Herausforderung für die Digitalisierung

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

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 entgegen zu wirken.

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 Digitalisierungs-barrieren aufgrund der DS-GVO aufzuzeigen und zu bewerten. Daraus könne Vorschläge und Maßnahmen abgeleitet werden, die dem erkennbaren Trend entgegen wirken und die wirtschaftliche Entwicklung der deutschen Wirtschaft zu stärken, sowie Wettbewerbsnachteile zu 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 (1)

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

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

Chart – BMWK Deutschland im internationalen Vergleich nur auf Platz 18 (3)

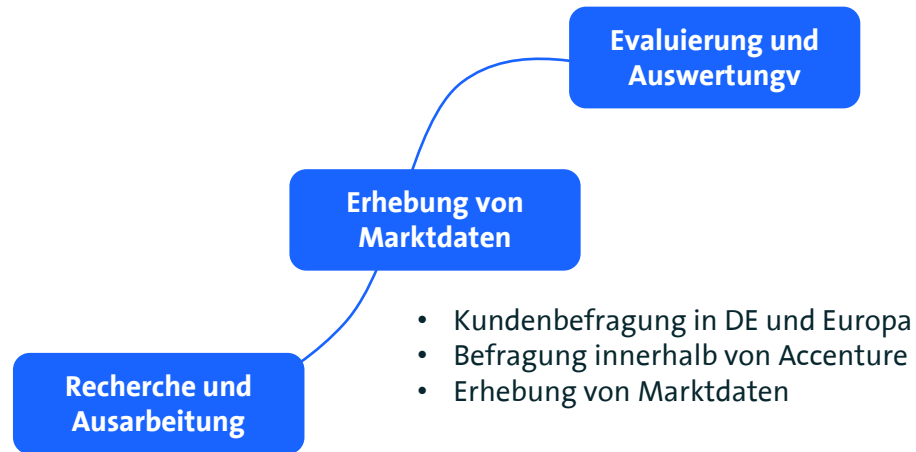


02

Methodik

Methodik

UNSER ANSATZ



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

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?

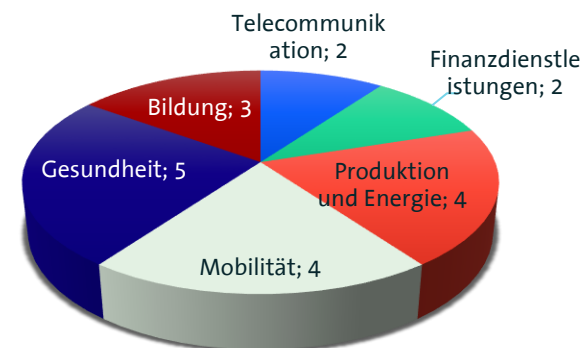
Finale Fragen

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

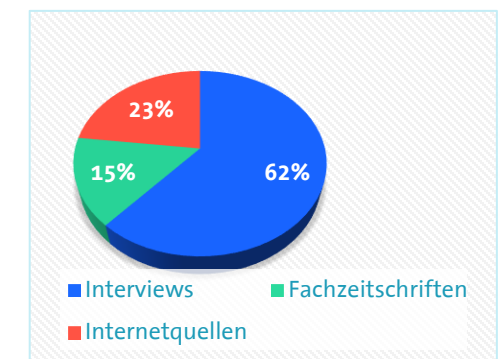
AUSWERTUNG

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

BETRACHTETE BRANCHEN



GENUTZTE QUELLEN



03

Ergebnisübersicht

Wichtigste Erkenntnisse

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

Auszug im Rahmen der Studie erhobener Anwendungsfälle:

Anwendungsfall: Office 365 an Schulen

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

Herausforderung	Aggregation	Interaktion
- Keine zentralisierte Verwaltung von Daten von Office 365 von Administratoren - Keine zentralisierte Verwaltung von Daten von Lehrkräften - Keine zentralisierte Verwaltung von Daten von Schülern - Keine zentralisierte Verwaltung von Daten von Eltern	- Keine zentralisierte Verwaltung von Daten von Lehrkräften - Keine zentralisierte Verwaltung von Daten von Schülern - Keine zentralisierte Verwaltung von Daten von Eltern	- Keine zentralisierte Verwaltung von Daten von Lehrkräften - Keine zentralisierte Verwaltung von Daten von Schülern - Keine zentralisierte Verwaltung von Daten von Eltern

Anwendungsfall: Smart Metering Systeme

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

Herausforderung	Aggregation	Interaktion
- Keine zentralisierte Verwaltung von Daten von Smart Metern - Keine zentralisierte Verwaltung von Daten von Verbrauchern - Keine zentralisierte Verwaltung von Daten von Netzbetreibern	- Keine zentralisierte Verwaltung von Daten von Smart Metern - Keine zentralisierte Verwaltung von Daten von Verbrauchern - Keine zentralisierte Verwaltung von Daten von Netzbetreibern	- Keine zentralisierte Verwaltung von Daten von Smart Metern - Keine zentralisierte Verwaltung von Daten von Verbrauchern - Keine zentralisierte Verwaltung von Daten von Netzbetreibern

Anwendungsfall: Impfstatusabfrage

DS-GVO verlangt eine vollständige Grundlage von Aufhebungen um den Impfstatus einer Arbeitnehmerin abzufragen. Eine solche gesetzliche Grundlage gibt es im Arbeits- & Sozialrecht aber nicht.

Herausforderung	Aggregation	Interaktion
- Keine zentralisierte Verwaltung von Daten von Arbeitnehmern - Keine zentralisierte Verwaltung von Daten von Arbeitgebern - Keine zentralisierte Verwaltung von Daten von Sozialversicherern	- Keine zentralisierte Verwaltung von Daten von Arbeitnehmern - Keine zentralisierte Verwaltung von Daten von Arbeitgebern - Keine zentralisierte Verwaltung von Daten von Sozialversicherern	- Keine zentralisierte Verwaltung von Daten von Arbeitnehmern - Keine zentralisierte Verwaltung von Daten von Arbeitgebern - Keine zentralisierte Verwaltung von Daten von Sozialversicherern

Anwendungsfall: Zentrales Cloud Computing

Kernanforderung Datenschutz (DS-GVO) sieht DS-GVO Anforderungen als nicht ausreichend an und sieht strikte Anforderungen auch für Cloud Computing vor.

Herausforderung	Aggregation	Interaktion
- Keine zentralisierte Verwaltung von Daten von Unternehmen - Keine zentralisierte Verwaltung von Daten von Cloud-Anbietern - Keine zentralisierte Verwaltung von Daten von Cloud-Nutzern	- Keine zentralisierte Verwaltung von Daten von Unternehmen - Keine zentralisierte Verwaltung von Daten von Cloud-Anbietern - Keine zentralisierte Verwaltung von Daten von Cloud-Nutzern	- Keine zentralisierte Verwaltung von Daten von Unternehmen - Keine zentralisierte Verwaltung von Daten von Cloud-Anbietern - Keine zentralisierte Verwaltung von Daten von Cloud-Nutzern

Anwendungsfall: App Entwicklung und Verbesserung

DS-GVO Anforderungen verlangen die Analyse von personenbezogenen Daten für die Effizienzsteigerung in Abläufen im Rahmen von Big Data-Analysen. Dadurch entstehen Wettbewerbsvorteile, hohe Kosten und rechtliche Risiken.

Herausforderung	Aggregation	Interaktion
- Keine zentralisierte Verwaltung von Daten von Apps - Keine zentralisierte Verwaltung von Daten von Entwicklern - Keine zentralisierte Verwaltung von Daten von Nutzern	- Keine zentralisierte Verwaltung von Daten von Apps - Keine zentralisierte Verwaltung von Daten von Entwicklern - Keine zentralisierte Verwaltung von Daten von Nutzern	- Keine zentralisierte Verwaltung von Daten von Apps - Keine zentralisierte Verwaltung von Daten von Entwicklern - Keine zentralisierte Verwaltung von Daten von Nutzern

Anwendungsfall: KI-Fahrerassistenz

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

Herausforderung	Aggregation	Interaktion
- Keine zentralisierte Verwaltung von Daten von Fahrerassistenzsystemen - Keine zentralisierte Verwaltung von Daten von Fahrern - Keine zentralisierte Verwaltung von Daten von Herstellern	- Keine zentralisierte Verwaltung von Daten von Fahrerassistenzsystemen - Keine zentralisierte Verwaltung von Daten von Fahrern - Keine zentralisierte Verwaltung von Daten von Herstellern	- Keine zentralisierte Verwaltung von Daten von Fahrerassistenzsystemen - Keine zentralisierte Verwaltung von Daten von Fahrern - Keine zentralisierte Verwaltung von Daten von Herstellern

Wichtigste Ergebnisse der Studie:



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 der Studie

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



Hohe Anforderungen der 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 innovativen 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 des bitkom

Auch diese Studie bestätigt, dass der Datenschutzrahmen zahlreicher Anpassungen bedarf



Um Deutschland zum führenden Daten- und Digitalstandort zu entwickeln bedarf es harmonisierter Auslegung und einer Umstrukturierung der Aufsichtsbehörden mit einheitlicher 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 bzw. angeglichen werden



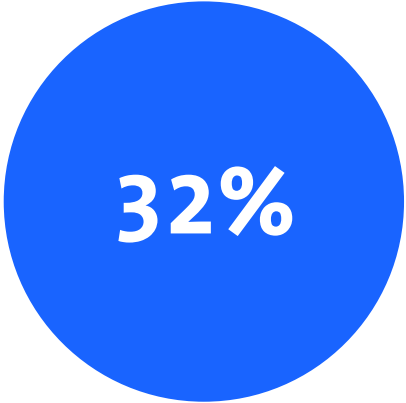
Deutschland sollte sich für stärkere Harmonisierung und einen kohärenten Rechtsrahmen in Europa einsetzen, um die Wettbewerbsverzerrung durch unterschiedliche Anforderungen zu minimieren



Das Dateninstitut sollte zu Datenkooperationen, Datenteilungsfragen beraten sowie den Aufbau von Kompetenzen fördern zB durch Data Scientist Ausbildungen

Zahlen und Fakten

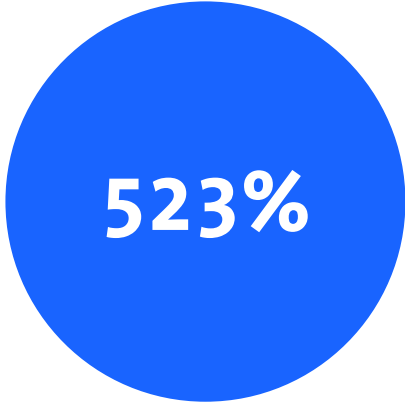
DS-GVO und Schrems II schaffen Unsicherheit bei Unternehmen.
Eine Klärung wäre dringend nötig!



32%

**Bedenken hinsichtlich der
Datensouveränität /
Rechtsvorschriften gehören zu den
größten Problemen bei der Cloud-
Einführung**

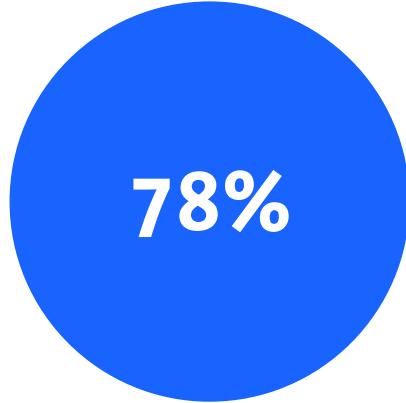
[Accenture. \(2021\). Keys to Cloud
Continuum Success](#)



523%

**Erheblicher Anstieg von Strafen
in 2021 im Vergleich zu 2020
- etwa 90 Mio Euro**

[CMS. \(2021\). DS-GVO Enforcement
Tracker](#)



78%

**Aller Unternehmen sehen
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
Datenschutzanforderungen 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

Berater für IT Sicherheit

"Datenschutz ist notwendig für Nachhaltigkeit."

KMU Eigentümer

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

Lösungsarchitekt

"Eine gesunde Sicherheitskultur ist fundamental."

Wirtschaftsanalyst

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

Manager für IT Sicherheit

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

Verkaufsberater

"Zu viel Regulierung beeinträchtigt die Wettbewerbsfähigkeit."

AI Ingenieur

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

Lösungsarchitekt

"Die Kluft zwischen Datenschutz und Technologie ist riesig."

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

Künstliche Intelligenz Potenzial, aber

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 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% fehlender Zugang zu externen Daten als große Herausforderung (2)
- Bereitschaft Daten zu teilen basiert auf Vertrauen auf sichere Datenverarbeitung
- Algorithmen der KI-Modelle sind transparent und nachvollziehbar, Mensch steht im Mittelpunkt
- Herausfordernd sind fehlende Ressourcen & resultierende Kosten (1)

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 ist gängige Praxis

Anwendungsfälle



KI-Fahrerassistenz



Smart Meters



Voice- & Chatbot



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 schaffen für die Erfüllung von Betroffenenrechten

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



SICHERHEIT D. VERARBEITUNG PRIV. BY DESIGN/DEFAULT

- Risiko-Analyse (ggfalls 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 72 h nach Erkennen reagieren zu können

- Meldung an die Behörde
- Ggfalls Mitteilung an betroffene Person
- Dokumentation



TRANSFER & AUFTRAGS-VERARBEITERVERTRÄGE

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



SPEICHERBEGRENZUNG & LÖSCHUNG

- Bildung von Datenarten
- Erhebung der Löschrufen
- 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

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

natürlich
juristisch

Räumlich ³



**ANWENDUNGS-
BEREICH**

GRUNDSÄTZE ⁵

- 1) Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- 2) Zweckbindung
- 3) Datenminimierung
- 4) Richtigkeit
- 5) Speicherbegrenzung
- 6) Integrität und Vertraulichkeit

RECHTMÄSSIGKEIT ⁶

- 1) Einwilligung ^{7 & 8}
- 2) Vertrag
- 3) Rechtliche Verpflichtung
- 4) Lebenswichtige Interessen
- 5) Öffentliches Interesse
- 6) Berechtigtes Interesse

> freiwillig gegeben
> in informierter Weise
> für den konkreten Fall
> unmissverständlich

> Für Kinder:
Zustimmung der Eltern

Rechenschaftspflicht

²DSGVO Artikel

RECHTE DER BETROFFENEN PERSON

> Transparente Information ¹²

- > knapp
- > einfache Sprache
- > verständlich
- > leicht zugänglich
- > transparent

Daten bei der betroffenen Person ¹³

> Bereitgestellte Information

Daten nicht bei der betroffenen Person ¹⁴

- > warum
- > was
- > wem
- > Drittland -> Garantien
- > wie lange
- > welche Rechte
- > vertraglich vorgeschrieben
- > automatisierte Entscheidung + Logik
- > andere Zwecke

> Auskunft ¹⁵

> Berichtigung ¹⁶

> Löschung = Recht auf Vergessenwerden ¹⁷

> Einschränkung ¹⁸

> Datenübertragbarkeit ²⁰

> Widerspruch ²¹

> Automatisierte Entscheidungen/Profiling ²²

Mitteilungs-
pflicht ¹⁹

> Beschränkungen ²³

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

- > 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)* ist eine europäische Verordnung der Europäischen Union, seit 25. Mai 2018 die Grundlage des allgemeinen Dateschutzrechts in der EU, und regelt die Verarbeitung personenbezogener Daten von EU-Bürgern, unabhängig von der Ansässigkeit des verarbeitenden Unternehmen.“

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 zusätzliche Aufmerksamkeit



Herausforderung

Der Hauptsitz der größten Cloud Anbieter befindet sich in den USA. Die regulatorischen Anforderungen an Unternehmen haben großen Einfluss z.B. DS-GVO, Cloud Act



Schrems II Urteil

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

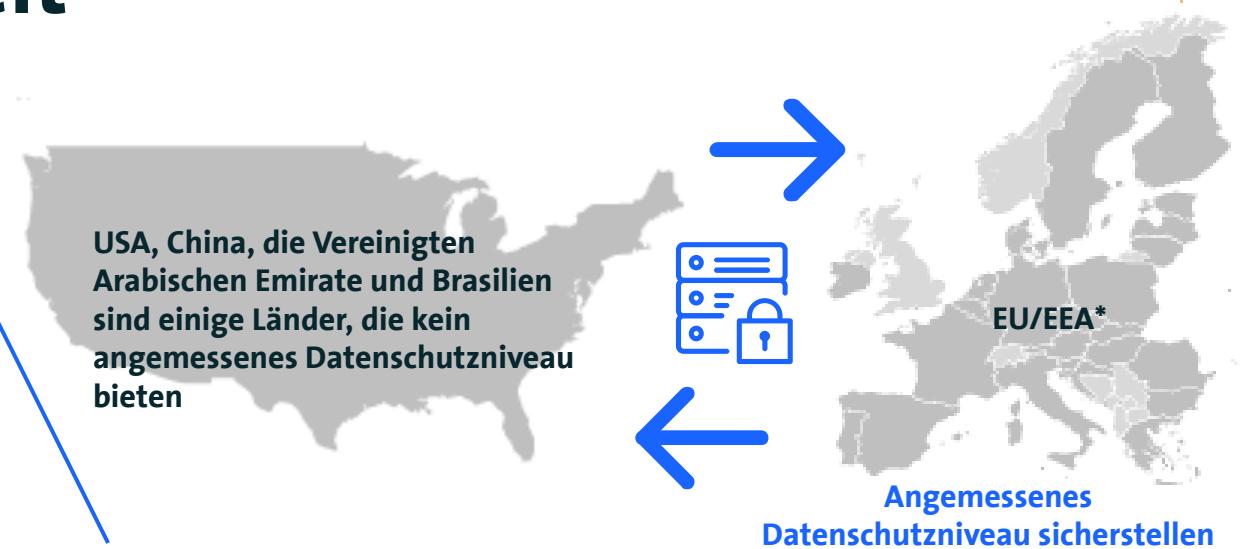


DS-GVO Anforderung

Eine Übermittlung personenbezogener Daten außerhalb der EU/des EWR darf nur vorgenommen werden, wenn dieses ein angemessenes Schutzniveau bietet (2)

*EU = European Union; EEA = European Economic Area

**DS-GVO, engl. GDPR = EU General Data Protection Regulation



NEWS

Rechtsunsicherheit bei der Nutzung von cloudbasierten Services wie jüngste nationale Entscheidungen zeigen:

- *deutsches Verwaltungsgericht verbietet Nutzung von US-Cookies (3)*
- *österreichische Datenschutzbehörde verbietet Google Analytics (4)*

Grund ist der Datentransfer in die USA.

Beispielhafte Übertragung personenbezogener Daten globaler Sicht

@Rebekka: aktuelle Daten verfügbar durch AVV Studie?

USA

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

+ Hohes Risiko

Hitzethermometer

- Niedriges Risiko

EWR und Länder mit Angemessenheitsbeschluss

In Überprüfung

Nicht anwendbar

Brasilien

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

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.

China

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

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 der **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.

05

Branchenüberblick und Anwendungsfälle

Übersicht der betrachteten Branchen

Im Rahmen der vorliegenden Studie wurden Anwendungsfälle aus folgenden Branchen herangezogen



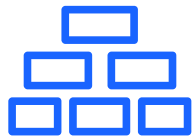
MOBILITÄT

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



BILDUNG

Bildungseinrichtungen von Schulen bis hin zu Universitäten und deren Nutzung von Services



FINANZDIENSTLEISTUNGEN

In die Finanzdienstleistungen fallen alle Dienstleistungen mit Bezug zu Finanzgeschäften, inclusive 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



Branche: Bildung

Unterschiedliche Positionen der lokalen Datenschutzbehörden führen zu einer großen Unsicherheit bei allen betroffenen Beteiligten, Schülern, Eltern und Lehrern, 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 personenbezogener Daten sein
- Cloud-basierte Angebote außerhalb der EU sind nur begrenzt nutzbar
- Verantwortlichkeiten sind nicht eindeutig geregelt e.g., Anbieter, Behörden
- Zustimmungsprozesse (Consent) für Anwender nicht transparent
- Unterschiedliche Aussagen sowohl national, als auch EU-weit
- COVID-19 als bedeutender Trigger (1)

Highlights

- Schwere geäußerte Bedenken bezüglich amerikanischen Anbietern durch Datenschutzbehörden
- Unterschiedliche Sichtweisen auf nationaler und internationaler Ebene

65%
der Lehrkräfte fühlen sich nicht ausreichend unterstützt bei Datenschutzfragen (2)

33%
der deutschen Schulen sind digitale Nachzügler (2)

57%
der Unternehmen produzieren e-Learning-Inhalte selbst ohne einen externen Dienstleister einzusetzen (3)

Anwendungsfälle



Videokonferenzdienste in Schulen



Office 365 an Schulen



Learning Analytics



Anwendungsfall: Learning Analytics im E-Learning

Mit Learning Analytics Technologien finden sich bereits in zahlreichen Lernmanagementsystemen wieder. Ein Beispiel ist die Moodle & iMOOC, wobei umfassende Pseudonymisierung nicht vollumfänglich gewährleistet werden kann und die Umgehung das vermeidliche Potenzial von Learning Analytics verpasst (1)

Marktforschung



Herausforderung:

- Ziel: Lernmuster erkennbar zu machen
- Verarbeitung von sensiblen Daten in digitaler Form aus Bildungskontext
- Verwendung von KI-Systeme erklärbar, transparent, & diskriminierungsfrei (1)
- Hürden/Angst um die Privatsphäre (9)



Rechtlich:

DS-GVO; Gesetze aus Bildungssektor; lokale Gesetze; Compliance RLs; *Trusted Learning Analytics* als Konzept für Ethik und Recht (2); 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 Datenspuren (3)

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 die Qualität und Wirksamkeit des Online-Lernens verbessern können (4)

Das Center of Data Innovation: hohen Kosten durch die Regulierung, daher kostet das KI-Gesetz die europäische Wirtschaft 31 Millionen €. KMUs, die Hochrisiko-KI-Anwendungen entwickeln, können mit 400 000 € rechnen und - 20% Investitionsvolumen wegen Compliance-Kosten

Rechtsinformatik-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 USA (9)
- Fehlende Arrondierung des Rechtsrahmens, daher Rechtsunsicherheit (2)
- Dies bedeutet, dass Rechtsfragen als Teil des Risikomanagements behandelt werden
- Aufgrund von den undurchsichtigen Sichtweisen, befinden sich Innovatoren im rechtsunsicheren Raum (8)

As Education Shifts Online, ClassDojo Serves 51 Million Students Worldwide. Announces Profitability and New 'Solo Capitalist' Funding

https://www.classdojo.com/privacycenter/

Privacy Center | ClassDojo

We are compliant with COPPA, FERPA, and GDPR in Europe. We will notify you if we make any changes to our practices. We're honored that tens of millions of you...

„ClassDojo“ überwacht Verhalten von Schülern

Mit der Gratis-App "ClassDojo" sollen Pädagogen eigentlich eine neue Möglichkeit zur Hand bekommen, ihre Schüler auf spielerische Weise zu einem positiveren Verhalten zu motivieren.

Quellen der Screenshots:
Computerwelt, ClassDojo überwacht Verhalten von Schülern; Pnewswire, As education shifts online ClassDojo servers 51 million students worldwide; ClassDojo, Privacy Center



Anwendungsfall: Office 365 an Schulen

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

Marktforschung



Herausforderung:

- Keine eindeutige Klärung, ob Einsatz von Office 365 rechtskonform ist
- Lokale Lernmanagementsysteme sind bescheiden
- 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, dass 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, dies gilt (4)

Bayerische DPA: Bei anderen Office-Anwendungen als Videokonferenz kann Pseudonymisierung in Betracht kommen (5)

Ministerium NRW: empfiehlt Logineo NRW (6)

OLG Frankfurt Urteil: Schulen in Hessen dürfen Office 365 weiterverwenden (7)

Bezirksregierung Arnsberg: Nutzung von Google-Diensten in Schulen verboten wegen Elternbedenken (8)

Fazit

- Lokale Lösungen scheitern landesweit (9)
- Derzeit stufen diverse staatliche Stellen (BW, NRW, Berlin, Bayern) die Nutzung von MS Office 365 als bedenklich ein. (3)(2)(6) Eine Prüfung ist sehr aufwendig und für die betroffenen Anwendergruppen intransparent
- Aufgrund von den 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 besonderen Zuspruchs der eingesetzten Produkte bleiben eine Vielzahl von Problemen und offenen Fragestellungen, welche weder das Kultusministerium noch die einzelnen Schulen datenschutzrechtlich verantworten können.

Wie sieht die datenschutzrechtliche Bewertung von Microsoft 365 für den schulischen Bereich aus?
Von der LfDI NRW ist mitgeteilt worden, dass ein bundesweiter, verbindlicher Vorgehensplan zur datenschutzrechtlichen Beurteilung von Microsoft 365 steht. Eine abschließende bundesweite, verbindliche Bewertung der Datenschutzanforderungen in Abstimmung mit Microsoft liegt noch nicht vor. Vor diesem Hintergrund müsste daher von der LfDI die Verletzung von personenbezogenen oder personenbezogenen Daten innerhalb von Microsoft 365 aktuell als datenschutzrechtlich bedenklich eingestuft werden. Das Schutzniveau empfiehlt daher, bei der Beschaffung und Nutzung von cloud-basierten Anwendungen auf das landesspezifische, zur Verfügung gestellte Angebot LOGINEO NRW für Datenspeicherung und E-Mail-Versand, auf LOGINEO NRW als Lernmanagementsystem sowie auf LOGINEO NRW Messenger mit integrierter Videokonferenzfunktion zurückzugreifen. Zudem ist künftig für LOGINEO NRW die Anbindung einer Office-Komponente vorgesehen.

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



Anwendungsfall: Videokonferenzdienste

Kollidierende 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 eine visuelle Brücke in Echtzeit zwischen Personen her. Dabei werden cloudbasierend Technologien genutzt und es kommt zur Übertragung von personenbezogene 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)

OLG Frankfurt Urteil: Vergabeverfahren wird gestoppt, folglich dürfen Schulen in Hessen Microsoft Team 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, welches Schulen Zeit und Geld kostet bzw. auch dazu führt, dass gewisse Features nicht mehr genutzt werden können
- Aufgrund von den unterschiedlichen Sichtweisen, können Betroffene nur schwer fundierte Entscheidungen treffen

Hessen: Gerichtsurteil stoppt Vergabeverfahren, Microsoft Teams bleibt



Quellen der Screenshots: [News4teachers](#), [Datenschutz an Schulen](#); [Das Windows 11 Magazin](#), [Hessen Gerichtsurteil stoppt Verfahren](#)



Branche: **Mobilität**

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

Herausforderungen

- Neue Technologien der Digitalisierung, wie AI und Cloud-Lösungen werden nur begrenzt eingesetzt
- Unterschiedliche nationale und international 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 führen zu unterschiedlichen Geschäftsmodellen in unterschiedlichen Regionen auch innerhalb der EU

2x

So hohe Kosten für
Ettiketierung
innerhalb der EU (1)

14. Platz

Deutschland im
Autonomous Vehicle
Readiness index (2)

€ 79 856 369

Von der Gesamtsumme
der im Transformations-
& Energiesektor
verhängten Geldbußen
(3)

Anwendungsfälle



KI-Fahrerassistenz



Personalisierte Preise



Risikoakzeptanz



Autonomes Fahren



Anwendungsfall: KI-Fahrerassistenz

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

Interview mit der Projektleitung



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 Labelling 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 Labelling 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 Europe 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: herausfordernd ist die immensen Datenmengen live zu verarbeiten, zu analysieren und zu speichern, um sie für Trainieren neuer KI-Software & 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 Politikern, Technikern, und Juristen im Bezug auf Wissensaustausch und Zusammenarbeit



Quelle von 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 von individuelle Preisgestaltung ist nicht geklärt (1)

Marktforschung



Herausforderung:

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



Rechtlich:

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

Technisch:

-



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 personenbezogene 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 Cookies gesammelten Informationen ändert. Auch lassen sich keine vergangenen DS-GVO Bußgelder finden

Personalisierte Preismodelle



Quelle von Screenshots: FAZ, Keine personalisierten Preise; help.ORF, Unterschiedliche Onlinepreise; BMJ, Schlussbericht bitkom



Anwendungsfall: DS-GVO Risikoakzeptanz

Nicht europäische Fluggesellschaft hinterfragt Anwendbarkeit und Durchsetzbarkeit der DS-GVO und trifft risikobasierte Entscheidung das Risiko von DS-GVO Bußgeld 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 diverse 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)

StandardDatenschutzmodell 2.0b: Risikoakzeptanz / -transfer steht wie in der Informationssicherheit nicht zur Verfügung. Restrisiko muss angemessen sein (2)

Datenschutzberater: 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 Platform in Frankfurt und Saint-Ghislain gespeichert werden (3)

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 ist die kostspieligen TOMs. So werden die Passengerdaten unter Umständen rechtsunsicher in Länder außerhalb der EU übertragen
- Aufgrund von den unterschiedlichen Sichtweisen, können Betroffene nur schwer fundierte Entscheidungen treffen



Quelle von Screenshots: Dr. DS-GVO, Ist Mailjet datenschutzkonform nutzbar?; Mailjet, Sicherheit & Datenschutz



Anwendungsfall: Autonomes Fahren

Die EU sucht nach einer Balance für Datensicherheit und Datenschutz sowie für 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

Marktforschung



Herausforderung:

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

Experten: Geforderte Sicherheitsausstattung bei Kleinwagen kostet etwa 1000 € pro Kfz (2)

Gartner: drahtlose Telematikgeräte und Black Box Technologien verarbeiten Daten Instandhaltung; Fahrzeugnutzung, und Wartungsbedarf (3)

Fazit

- Bekannte Autohersteller setzen statt auf Digitalisierung und Technologieoffenheit eher auf Implementierung von Datenschutzlösungen für Kunden
- Die Diskrepanz steigt zwischen der Verarbeitung von Datemengen für KI Modelle und Datenschutz im Auto (3)
- Der Datenschutz wird immer mehr in Industriestandards miteinbezogen ua auch in den TISAX





Branche: Gesundheit

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 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
- Statusabfrage durch den Arbeitgeber beschränkt möglich

Highlights

- Unterschiedliche Corona Apps in verschiedenen Ländern und Regionen mit bescheidenen Anerkennungen
- Einschränkungen von Gesundheitsservices
- Rechtsunsicherheit bei Anwendbarkeit

1.8 Million

Downloads der
CovPass App in
Deutschland (2)

€ 12,510,933

Gesamtsumme der
Geldbußen in der
Gesundheitsbranche
(3)

79

Gesamtzahl der
verhängten Geldbußen
in der Gesundheit (3)

Anwendungsfälle



Corona Apps



Fitness Apps



**Impfabfrage durch den
Arbeitgeber**



TraumaRegister DGU®



Anwendungsfall: Corona Contact Tracking Apps

Digitale automatisierte Kontaktverfolgung durch Mobile Contact Tracing Applikation am Smartphone.

Beispiele sind die Stopp-Corona App vom Rotes Kreuz, Novid20 (1), und 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 EMRK (2)



Technisch:

Entwicklung mittels Kontakterkennung über ein automatisches Pairing per Bluetooth, welches bei anonym die betroffenen Personen benachrichtigt (6)

Argumentation

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, Einschränkung Handlungsfähigkeit ohne Appinstallation, oder durch 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** Bluetooth statt auf Geolokalisierung setzen (5)

Fazit

- Entwicklung der Handyapplikationen binnen weniger Wochen, um die Ausbreitung von COVID-19 flott einzudämmen
- Organisationen mussten bei App Entwicklung in kurzer Zeit die DS-GVO Anforderungen interpretieren und implementieren, um keine Strafe zu riskieren
- Die unklaren Umsetzungsansichten erschwert erschwert DS-GVO Konformität und verlängert Prozess der App Entwicklung



Quelle Screenshots: [StoppCorona](#), [FAQ](#); [Accenture](#), [Stopp Corona-App](#)



Anwendungsfall: Corona luca app

Neben den „normalen“ Kontaktverfolgungsfeatures und Risikokontaktbenachrichtigung mit kritisch-gesehenem Geofencing, hat die luca app auch einen wirtschaftlichen Nutzen

Marktforschung



Herausforderung:

- Digitale automatisierte Kontaktverfolgung via App mit wirtschaftlichem Nutzen (!) wie Gästeregisterierung, Kontakttagebuch, Kontaktnachverfolgung mit Anbindung an Gesundheitsämter (1)
- Verarbeitung personenbezogener Daten und sensibler Gesundheitsdaten



Rechtlich:

Artikel 6, 9, 25 DS-GVO



Technisch:

Entwicklung Erkennung über ein automatisches Pairing. Luca erstellt einen persönlichen, sich ständig ändernden und verschlüsselten QR-Code (6)

Argumentation

Verbraucherzentrale: luca app sammelt im Gegensatz zur Corona-Warn-App personenbezogene Daten bei aktiver Nutzung e.g., auch 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-Sicherheitsforschern: Luca app erfüllt nicht dieselben Prinzipien wie die Corona Warn App, da es u.a. keine technische Zweckbindung gibt, sondern Gewinnabsicht Privater besteht oder aufgrund des Designs Missbrauchrisiko besteht (4)

Bayerische Staatsministerin 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 (CCC, Gesundheitsämter, 70 führende deutsche IT-Sicherheitsforscher, usw.)
- 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 zu was ist erlaubt und was nicht, wird es den Betroffenen erschwert innovative Projekte zu umzusetzen



Quelle Screenshots: [luca app](#)



Anwendungsfall: TraumaRegister DGU®

Health Research gehemmt! DGU behauptet übertriebener Datenschutz gefährdet Menschenleben in der Schwerverletztenversorgung

Marktforschung



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 Patienten (1)



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, aber zunehmen auch weitere Länder (2)

Argumentation

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

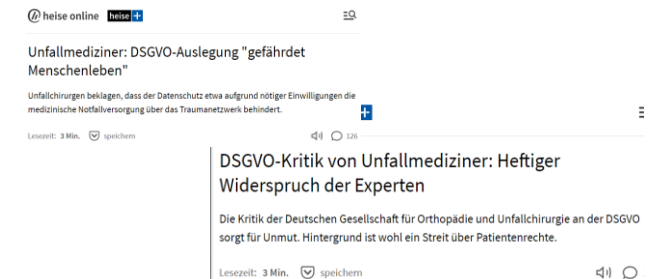
DGU-Präsident: „Aber übertriebener Datenschutz macht unser seit fast 30 Jahren bestehendes TraumaRegister nun zunichte und gefährdet damit Menschenleben“ (1)

Grünen-Poliker 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 vorsieht (5)
- Der Fall zeigt Unsicherheit und Spielraum für Missinterpretation der DS-GVO bzw. das Unverständnis für Fehlinterpretationen



Quelle Screenshots: [Heise Online](#), Unfallmediziner; [Heise Online](#), DSGVO-Kritik



Anwendungsfall: Impfstatusabfrage

DS-GVO verlangt eine rechtliche Grundlage von Arbeitgebern um den Impfstatus seiner Arbeitnehmer obligatorisch zu erfassen. Eine solche gesetzliche Grundlage gibt es im Arbeits- & Sozialrecht aber nicht

Marktforschung



Herausforderung:

- Frage um die Impfstatusabfrage des Arbeitnehmers durch den Arbeitgeber
- Informationen über den Impfstatus sind ebenso Gesundheitsdaten wie das Corona Testergebnis bzw. Nachweis einer überstandenen Infektion
- Diese stehen unter besonders strengem Schutz der DS-GVO (2)



Rechtlich:

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



Technisch:

-

Argumentation

Bundesministerium für Gesundheit:

Die Auskunftspflicht gilt nur für 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, nämlich aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit

Datenschutzkonferenz: In Ermangelung einer gesetzlichen Grundlage bedarf es in der Regel einer Einwilligung der Arbeitnehmer 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 somit einzelfallabhängig geprüft werden
- Das lässt sich durch Rechtsklarheit und eine einheitliche Lösung erreichen, was im Moment nicht der Fall ist (2)



Der große Wurf, den sich die Arbeitgeber wünschen, ist vom Tisch: Union und SPD einigen sich in der Debatte um die Impfabfrage durch Arbeitgeber. Bestimmte Berufsgruppen müssen ihren Impfstatus offenlegen.

VON CHRISTIAN GENITZ, BERLIN - AKTUALISIERT AM 01.09.2021 - 08:08

(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;

Quelle von Screenshots: FAZ, Einigung zur Abfrage des Corona-Impfstatus durch Arbeitgeber



Anwendungsfall: Mobile Health Apps

Smartphone nutzer können weder die automatische Messungen ihrer mobilen Health Apps nicht abschalten, noch die Applikationen entgültig vom Smartphone deinstallieren – Grauzone: Was ist erlaubt und was nicht?

Marktforschung



Herausforderung:

- Datenschutzbedenken bei gesundheitsbezogenen Apps wie Apple Health (iOS) und Google Fit (Android)
- Apps sammeln sensible Daten von Nutzern, meist automatisch
- Apps lassen sich nicht vom Endgerät deinstallieren
- Unklar ist der Datenaustausch mit anderen Apps untereinander (1)



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 mHealth-Apps: Google bietet einen Großteil seiner Produkte kostenlos an, mit dem Ziel Daten sollen wie Rechnungen, Dokumente, Gesundheitsdaten oder Videos ablegen. Google ist einer der größten Werbeplattformen (3)

Aspekte zu Apple Health: Daten werden lokale gespeichert & verschlüsselt, aber Nutzer können Messungen nicht abschalten, noch ist der Datenaustausch transparent (2)

Aspekte zu Google Fit: keine besonderen Schutzvorkehrungen, kommerziell getriebene Kooperationen, und automatische Messungen (2)

Fortune Business Insights: die COVID-19 Situation führte 2020 zu einem Wachstum von 66 % an Downloads von mobilen Health Apps (4)

Europäische Kommission: Ein Verhaltenskodex soll das Vertrauen der Nutzer fördern und einen Wettbewerbsvorteil verschaffen (5)

BVDW: Faktencheck über 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 dem Nutzer oft nicht transparent
- Nutzer können nicht selber über Messung durch Smartphone entscheiden
- DS-GVO lässt mehrere Öffnungsklauseln für den öffentlichen Sektor und Gesundheitswesen (1)

Europäische Kommission
Datenschutzbeauftragter, Mr.
Johannes Wirth
Rechtsanwältin, Dr. Ingrid
Mayer
März 2020

Datenschutzrechtliche Problematik von
mHealth-Apps und Wearables im Bezug
auf das europäische und österreichische
Datenschutzrecht.



Quelle Screenshots: IKU, Datenschutzrechtliche Problematik von mHealth-Apps und Wearables.docx;



Branche: Produktion und Energie

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

Herausforderungen

- Fokus von Produktionsunternehmen liegt auf Prozessen der Wertschöpfungskette, kein People-Business (1)
- Risikomanagement von Cloud-Lösungen in Produktionsbranche bescheiden (2)
- Die Energiebranche zählt zur kritischen Infrastruktur und unterliegt besonderen lokalen und europäischen Regularien
- Verarbeitung besonders sensible personenbezogene Daten e.g., **Stromverbrauch, Name, Adresse** (3)

Highlights

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

17%
der dt. Bevölkerung
hat Smart Meter
installiert (4)

€ 53 341 369
Gesamtsumme der
Geldbußen im
Transport &
Energiesektor (5)

43
Gesamtanzahl der
Geldbußen im Transport
& Energiesektor (5)

Anwendungsfälle



US Cookietransfer



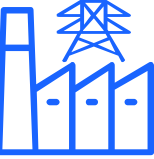
Datenmigration



Smart Meters



Kundenverhalten



Anwendungsfall: US Cookietransfer

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

Marktforschung



Herausforderung:

- Mit dem dänischen Cookiebotanbieter Cybot, können Websitebetreiber ihre Besucher um Einwilligung zur Speicherung von Cookies ersuchen
- Verarbeiter hatten nicht notwendigen Maßnahmen nach Schrems II ergriffen
- Datenübertragung von Websitenutzern zu US Servern nur mit besonderer vorheriger Absicherung (1)



Rechtlich:

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



Technisch:

Mit Cookiebanner können Websitenutzer 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 reCAPTCHA, Google Analytics (1)

Angeklagter Hochschule RheinMain: Standardvertragsklauseln liegen vor. Cybot werde nur "anonymisierte" Internetkennung, Datum und Uhrzeit der Zustimmung, Nutzeragent des Browsers, URL, anonymer, zufälliger & verschlüsselter Schlüssel und Einwilligungsstatus übermittelt (1)

Hessischer Datenschutzbeauftragter: bestätigt die Verarbeitung von Klardaten mit bloßer Transportverschlüsselung und damit keine ausreichenden Schutzmaßnahmen vorliegen (1)

Fazit

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

Gericht: Deutsche Webseiten dürfen keine US-Cookies setzen

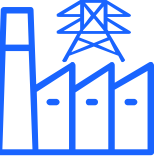
Das Verwaltungsgericht Wiesbaden untersagt einer Hochschule, auf ihrer Webseite den "Cookiebot" einzusetzen. Der gesetzliche Beschluss wirkt weit.

Lesen Sie: 2 Min. | 100 Wörter



Cookiebot

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 war fehlende Datenklassifizierung und Aufwand, personenbezogene und auch sensible Daten zu trennen und schützen, basierend auf DS-GVO Anforderungen

Interview mit der Projektleitung



Herausforderung:

- Datenmigration von einer alten On-Premise Infrastruktur zu einer neuen bzw. in die Cloud
- Externe 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 ordnungsgemäß durch externe Berater in die neue Umgebung zu migrieren

Argumentation

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

Sewobe : Fehler passierend schnell und können riesige Schäden anrichte e.g., verlorene personenbezogene Daten (1)

Talend: bei Erstellung des Datenmigrationskonzepts sollte Kenntnis über Daten vorliegen (2)

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

Fazit

- Erhöhung des Projektbudgets und –zeit durch die Einbeziehung von Spezialisten und zusätzlicher Technologie
- Druck auf Qualität und Genauigkeit (4)
- Die DS-GVO bewirkt eine Umstellung des Datenmanagements, Datenschutzkonzepte und zusätzliche organisatorische und technische Maßnahmen, auch wenn Anwendungsfälle dies nicht erfordern

NEWS

Focus: SAP S/4Hana Transformation

SAP S/4Hana-Migration: Kosten schlechter Stammdaten vermeiden

11.10.2021 - 08:45 Uhr
von Matthias Fiedt, Head of Sales, Unitary

Unternehmen kommen nicht umhin, eine Migration zu SAP S/4 anzustreben, denn der Herstellersupport für Alt-Systeme ende 2020. Richtig umgesetzt, birgt die Migration wertvolle Chancen das weitere Datenmanagement und kann sogar Kosten sparen. Dieser Beitrag liefert Tipps für eine gelungene Umsetzung.

More than a data move

It is vital that on-premise or legacy systems and the cloud system work in harmony, especially when it comes to payroll. Here are some essential considerations when moving data from one system to another.

Validation is fundamental before, during and after migration

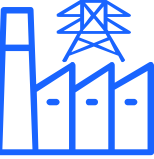
All HR teams want to focus closely on the task in hand—making sure data is available and in the right system. But moving data to the right place is only one part of the migration challenge. If it is found to be inaccurate or incomplete, that migration is far from being a success.

Validation can measure HR users that they are handling accurate, up-to-date data. But it is one of those tasks that is often overlooked.

Regulation puts pressure on quality and accuracy

The heat is on as a result of European Union General Data Protection Regulation (GDPR) and other relevant and upcoming legislations. HR professionals cannot focus on just one data segment, they need to tackle it all holistically. The ASUG survey finds that most companies feel that compliance measures (such as GDPR) will at least somewhat affect data handling processes going forward.

Quelle Screenshots: (3) und (4)



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 Verbrauchswert des Energieverbrauchs
- Diese stellen personenbezogene Daten dar und Bedenken umfassen Profiling, mangelnde Kontrolle, IoT-Geräte Risiken, 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 Meters/intelligentes Stromzählen messen den Energieverbrauch und stellen diesen Verbrauchswert täglich dem Netzbetreiber über eine Kommunikationsanbindung zu Verfügung

Argumentation

Minister in Schleswig-Holstein: Wir brauchen das Mgmt. 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

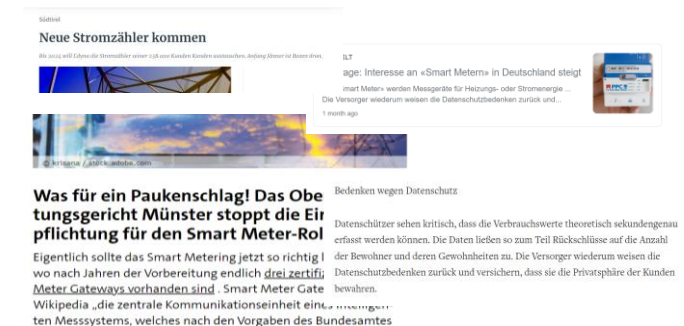
Minister in Brandenburg: Bundespolitik sollte die nötigen Rahmenbedingungen für Energiewenden schaffen. Das Genehmigungsverfahren sei eine Katastrophe e.g., Übertragungsnetzleitung Uckermark läuft seit 16 Jahren und beim Breitbandausbau sieht es ähnlich aus (1)

Urteil des nordrhein-westfälisches OVG: Smart Metering darf nicht eingesetzt werden (2)

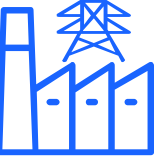
Generaldirektor von Edyna - größter Stromverteiler Südtirols: Smart Meter ist als wichtige Innovation, die unser Stromnetz noch intelligenter & digitaler macht. Dadurch können wir Energieverteilung effizienter steuern und Servicequalität verbessern. Edyna will bis 2024 Stromzähler mit Smart Metern ersetzen (3)

Fazit

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



Quelle Screenshots: Umfrage: Interesse an «Smart Metern» in Deutschland steigt; Was für ein Paukenschlag! News-Blog der datenschutz nord Gruppe; (3)



Anwendungsfall: Kundenverhalten

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

Marktforschung



Herausforderung:

- 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



Technisch:

-

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 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 ein Graubereich der DS-GVO darstellt
- Für Unternehmen ist der Umfang der Transparenzpflicht nach DS-GVO unklar
- Folglich akzeptiert das Unternehmen die Sanktion und erweitert mit der Behörde die „notwendigen Angaben“



Quelle Screenshots: [Europe.eu](#), Hamburg DPA; [Datenschutz-Hamburg, Bußgeld gegen Vattenfall](#)



Branche: Telekommunikation

Bei fast 90% personenbezogener Daten 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 im Vergleich zu vor der Einführung DS-GVO für Datenschutzthemen

Herausforderungen

- Stark reglementierter Geschäftsbereich (TKT, DS-GVO, ITSG)
- Das Geschäftsmodell baut auf Kommunikationsangeboten auf
- Sammeln viele persönlichen Daten e.g., Navigation, Adresse, Call Data Records
- Internationale Zusammenarbeit durch interne / externe Kooperationen e.g., Abschluss von AVV, Datenübertragung
- Rechtsunsicherheit trotz behördlichem Review. DPO sucht Klarheit, um Grauzonen der DS-GVO zu meiden

Highlights

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

2ter Platz
der Anzahl verhängter
Geldbußen (1)

€ 369,724,441
Gesamtsumme
verhängter
Geldbußen (1)

159
Gesamtanzahl
verhängter
Geldbußen (1)

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 von personenbezogenen Daten für die Effizienzsteigerungen in Abläufen im Rahmen von Big Data Analysen. Dadurch entstehen Wettbewerbsnachteil, hohe Kosten, und nichtgenutzte Qualitätspotenziale der entwickelten Anwendungen

Interview mit der Projektleitung



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 ermöglicht eine enorme Effizienzsteigerung und Strukturierung bestehender Abwicklungsprozesse. Dadurch können signifikante Einsparungen und kürzere Bearbeitungsprozesse ermöglicht werden

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

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

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

Fazit

- Kosten für Ressourcen in Europa sind kostspieliger als in e.g., 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 welche Maßnahmen notwendig und geeignet sind
- Übermittlung ins Ausland ist nicht möglich und verhindert so die Qualität dieser Daten. Adoptionen sind kostenintensiv



Branche: Finanzdienstleistungen

Die Finanzbranche stellt sich der Herausforderung der besonders hohen Regelungsdichte, gleichzeitig konzentrieren sich hier besonders viele Big Data Projekte. Trotzdem kämpfen ~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/Banken
- Sicherheit, Datenschutz, Compliance haben oberste Priorität (2)
- Einsatz innovativer Technologien wie Cloud Computing und AI notwendig, um Wettbewerbsfähig zu bleiben
- Banken haben detaillierte Einblicke in das Leben seiner Kunden (3)

Highlights

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

Anwendungsfälle



Cloud Solution



Voice- & Chatbot

Jedes 8te

Unternehmen fehlt es an konkr. Zielen bei Implementierung innovativer Technologien (1)

€ 28,356,065

Gesamtsumme der Geldbußen für Finanzen, Versicherungen, und Beratung (4)

93

Gesamtanzahl der Geldbußen für Finanzen, Versicherungen, und Beratung (4)



Anwendungsfall: Zentrales Cloud Computing

Koreanisches Datenschutzgesetz (PIPA) sieht DS-GVO Anforderung 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 eine Projekt über einen zentralisierten Cloud-Ansatz für eine globalen Verwaltung



Rechtlich:

DS-GVO; PIPA (koreanisches Datenschutzgesetz)



Technisch:

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

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 Produktionbranche nach Kritikalität und die Finanzdienstleistungsanbieter haben Verständnis & Awareness für Security und Privacy Requirements

Jedes Land hat eigene Anforderungen e.g., Russland setzt voraus ummer eine unverschlüsselte Kpie in Russland zu lassen, während China sogar verlangt, dass eine lokale Kopie in auf chinesischen Servern gespeichert werden muss

Fazit

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



Quelle der Flaggen ist das Accenture BrandSpace repository



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 vieler Big Data für effektive Bots
- Algorithmische Transparenz
- Einwilligung der Nutzer
- Modellentwicklung aus gesammelte Daten versus Recht auf Löschung. Datenminimierung bedingt möglich, da alle Daten angegeben werden könnten



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 bei komplexeren Anfragen an Menschen weiterzuleiten (1)

Argumentation

DZ CompliancePartner: werden personenbezogene Daten verarbeitet, sind zahlreiche Anforderungen aus der DS-GVO zu beachten, daher u.a. Einholung der Einwilligung des Kunden, Datenschutz-konweise, Löschung, Verschlüsselung (4)

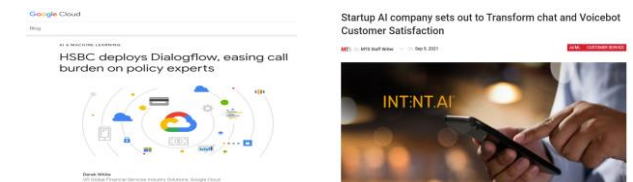
Business Analyst Interviewee: Der Einsatz ist möglich, aber Chatbot-Anbieter müssen Datenschutzregularien frühzeitig im Projekt berücksichtigen und eine unternehmensweite Strategie entwickeln, mit menschlichen Agenten kombinieren, strenge Benutzerakzeptanztests durchführen und Schulungen für Mitarbeiter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

Insider Intelligence: 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 Unternehmensservice-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 apriori der Markteinführung
- Datenschutzgesetze in Europe werden stikt ausgelegt, viele Einschränkungen (6)



Quelle des Screenshots: [Google Cloud Blog](#), [MTS](#), [Startup AI company sets out to Transform chat and Voicebot Customer Satisfaction](#)

06

Limitationen und Bibliographie

Limitationen der Studie

Ausgangssituation:

Wie bei jedem Forschungsprojekt, handelt es sich bei der vorliegenden finalen 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 Autoren sind sich voll und ganz bewusst, dass der entwickelte Kontext verschiedene selektierte Anwendungsfälle und Branchen darstellen soll und mit Potential 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 umfassen u.a.:

- Der geografische Umfang der Studie umfasst Europa mit dem Fokus auf Deutschland. Die Anwendungsfälle und Branchenerklärungen 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 Imputdaten 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 Innovation- 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⁾

(1) bitkom, Digitale Prozesse Begriffsabgrenzung und thematische Einordnung, S 8

Alle Interviews wurden manuell protokolliert und in ein Excel eingepflegt, jeweils der passenden Frage und Antwort

Describe your Role	What kind of barriers can you identify within 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
- Since Feb 2021 with acn - Bank, insurance companies, digitalization projects (data warehousing, ...) - Banking and finance background	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 e.g., much more hesitant to move into AWS cloud since this constitutes a data transfers to a third party Bc of this for banks is harder to make use of	Big European Bank: 2 projects 1) improve data warehousing / data mgmt: transfer of confidential client information from one legal entity to another 2) chat-voicebots: automated answering machine for questions of clients / potential clients (basically everyone) over the internet, with the goal not to have to communicate to a real person	Big European Bank: 2 projects 1) Ensure data data is scrapped 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
7 years in Accenture, mainly in SAP platform security domain.	The barriers are more conceptual. Identifying data and making the client aware of the importance of data is a challenge.	Big German Chemical company - Big German automobile company Manufacturing company	Bringing specialist into the project to help clients identify the critical data that need to be protected.

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 Bitcom. (2016). Digitale Prozesse. Begriffsabgrenzung und thematische Einordnung. <https://www.bitkom.org/sites/default/files/file/import/160803-Whitepaper-Digitale-Prozesse.pdf>

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

Bibliographie

Fachspezifische Referenzen

Bildung

- 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
- 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>

Bibliographie

Fachspezifische Referenzen

Bildung

- 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>

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. Dezmeber 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

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-grenzuberschreitende-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)
- 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
- 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)

Bibliographie

Fachspezifische Referenzen

Gesundheit

- 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). EntschlieÙung 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

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)

Bibliographie

Fachspezifische Referenzen

Produktion und Energie

- 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 Krampfl. (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 Stronzähler kommen. <https://www.rainews.it/tgr/tagesschau/articoli/2021/12/tag-edyna-neue-stromzaehler-smart-meter-d1da1f87-808f-424f-97d9-e824467688d7.html>
- 11 Stefan Krempl. (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>

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/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>

07

Team

Ihr Projektteam

Bitkom e. V.
Albrechtstraße 10
10117 Berlin
bitkom.org



Susanne Dehmel
Mitglied der Geschäftsleitung Recht & Sicherheit
Bitkom e.V.
s.dehmel@bitkom.org



Rebekka Weiß
Leiterin Vertrauen & Sicherheit
Bitkom e.V.
r.weiss@bitkom.org / +49 15117439698

Accenture
Campus Kronberg 1
61476 Kronberg im Taunus
www.accenture.de



Raimund Wilhelmer
Principal Director Security Innovation
Accenture
raimund.wilhelmer@accenture.com



Prithwi Lahiri
Security Consulting Consultant
Accenture
prithwi.lahiri@accenture.com



Doris Winkler
Security Consulting Analyst
Accenture
doris.winkler@accenture.com