

T.I.S.P. Community Meeting 2023

Berlin, 07. - 08.11.2023

Datenschutz als Wettbewerbsvorteil und Wettbewerbsnachteil

Friederike Schellhas-Mende, Secorvo Security Consulting GmbH

A photograph of a chessboard with various pieces (kings, queens, knights, pawns) arranged on it. The background is blurred, showing people in a social setting. A semi-transparent dark red banner is overlaid on the bottom half of the image, containing the title text.

Datenschutz als Wettbewerbsvorteil und Wettbewerbsnachteil

T.I.S.P. Community Meeting 2023

Berlin, 06.11.2023

Friederike Schellhas-Mende

Wer ich bin?



Friederike Schellhas-Mende

Volljuristin

Warum dieser Vortrag?

Wie wird Datenschutz wahrgenommen?

Handelsblatt

tschland > Mehrheit deutscher Firmen sieht durch strengen EU-Datenschutz keinen Wett

IW-Studie zur DSGVO

Mehrheit deutscher Firmen sieht EU-Datenschutz nicht als Vorteil im Wettbewerb

Nur wenige deutsche Unternehmen glauben, sich mit einem starken Datenschutz einen Wettbewerbsvorteil

WirtschaftsWoche

UNTERNEHMEN FINANZEN ERFOLG COACH POLITIK TECHNOLOGIE WiWo+ Alle Rubriken

Top-Themen | WiWo > Politik > Konjunktur > DSGVO & Co.: Übertriebener Datenschutz ist ein Wettbewerbsnachteil

WIRTSCHAFTS WOCHE EINGESPERRTER DATEN-SCHATZ

Wenn übertriebener Datenschutz zum Problem für die Forschung wird

von Bert Losse
10. Januar 2023

SWR >> Suchen

SWR Fernsehen / Zur Sache Baden-Württemberg

Wird der Datenschutz übertrieben?

Stand: 15.12.2022, 21:17 Uhr



ZUR SACHE!
BADEN-WÜRTTEMBERG

Teilen:   

ehen unseren Datenschutz als Wettbewerbsnachteil.

Neue Datenschutz-Grundverordnung

Sollte ich meine Webseite besser ABSCHALTEN?



Wer schützt mich vorm Datenschutz?
Foto: coremedia

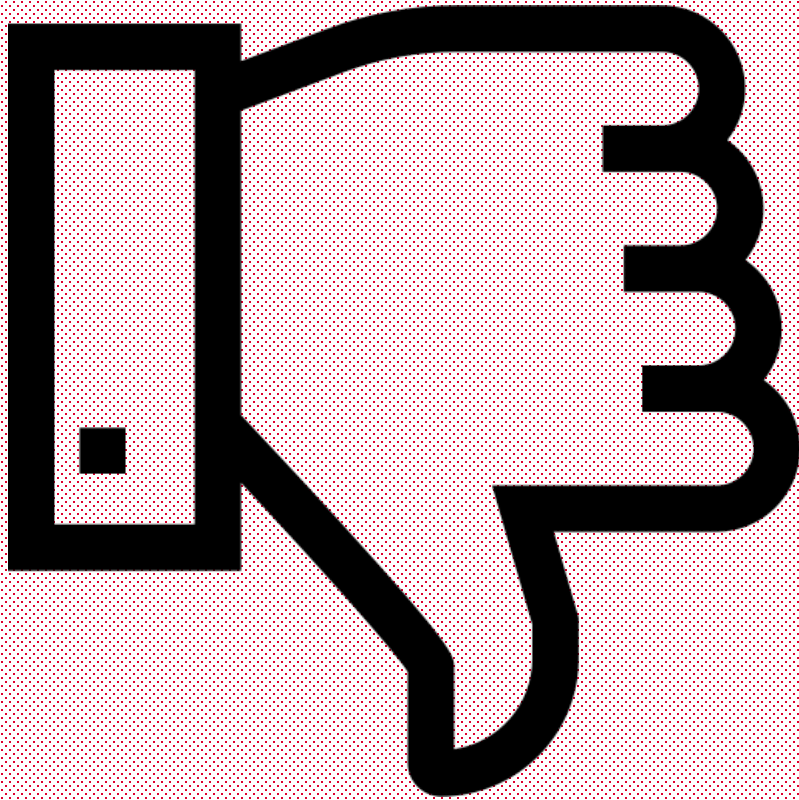
bitkom

Zweifelsfragen um die informationelle Selbstbestimmung - Datenschutz als Datenaskese?*

Presseinformation

DS-GVO bringt nur den wenigsten Unternehmen Wettbewerbsvorteile

Datenschutz nervt!?



Ist Datenschutz ein Wettbewerbsnachteil?

Wann ist Datenschutz tatsächlich ein Wettbewerbsnachteil?

- Wenn Innovationen nicht vorangetrieben werden auf Grund von Datenschutzbedenken.
- Wenn Datenschutzmaßnahmen nicht umgesetzt werden, auf Grund des befürchteten Aufwands.
- Wenn Datenschutz nur partiell und nicht konsequent umgesetzt wird.

It's a classic...Beispiele für Missverständnisse/ Ausreden/ Ängste

Sie dürfen hier nicht fotografieren, wegen (dem) Datenschutz“

„Sie müssen in die Datenschutzerklärung einwilligen, sonst können wir nicht behandeln.“

- Frage der Anwendbarkeit der DSGVO (-)
- Verbot ergibt sich aus dem Hausrecht, nicht wegen des Datenschutzes
- Einwilligung wegen des Rechts am eigenen Bild erforderlich, Ausnahme bei Kindern und bei Veröffentlichung der Bilder.

<https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/09/Fotografieren-und-Datenschutz-September-2019.pdf>

- In Datenschutzerklärungen muss man nicht einwilligen, sie dienen der Information der Betroffenen.
- Einwilligungen braucht man dann, wenn es keine andere Rechtsgrundlage z.B. Vertrag gibt.
- Über die Datenverarbeitung muss informiert werden.

Cookie-Banner-Wahnsinn

RP-BW > Themenportal > Gesellschaft > Schule und Bildung > Richtlinien an Schulen > Unterricht > Fach

Hinweis zu Cookies

Um unseren Internetauftritt für Sie optimal gestalten und verbessern zu können, verwenden wir Cookies. Weitere Informationen zu Cookies erhalten Sie in unserer **Datenschutzerklärung**.

Erforderlich

[Drittanbieter-Cookies](#)

Akzeptieren Alle Cookies akzeptieren

Cookie-Zustimmung verwalten

Wir verwenden Technologien wie Cookies, um Geräteinformationen zu speichern und darauf zuzugreifen. Wir tun dies, um das Surferlebnis zu verbessern und (nicht personalisierte) Werbung anzuzeigen. Wenn Sie diesen Technologien zustimmen, werden wir Daten wie das Surfverhalten oder eindeutige IDs auf dieser Website verarbeiten. Ihre Nichteinwilligung oder der Widerruf der Einwilligung kann sich nachteilig auf die Funktionalität und Merkmale der Website auswirken.

[Dienste verwalten](#)

Akzeptieren Leugnen Open

[Cookie-Richtlinie](#)

Datenschutz & Transparenz

Wir und unsere Partner verwenden Cookies, um Informationen auf einem Gerät speichern und/oder abrufen zu können. Wir und unsere Partner verwenden Daten für Personalisierte Anzeigen und Inhalte, Anzeigen- und Inhaltsmessungen, Erkenntnisse über Zielgruppen und Produktentwicklungen. Ein Beispiel für Daten, welche verarbeitet werden, kann eine in einem Cookie gespeicherte eindeutige Kennung sein. Einige unserer Partner können Ihre Daten im Rahmen ihrer legitimen Geschäftsinteressen verarbeiten, ohne Ihre Zustimmung einzuholen. Um die Verwendungszwecke einzusehen, für die diese Ihrer Meinung nach ein berechtigtes Interesse haben, oder um dieser Datenverarbeitung zu widersprechen, verwenden Sie den unten stehenden Link zur Anbieterliste. Die übermittelte Einwilligung wird nur für die von dieser Webseite ausgehende Datenverarbeitung verwendet. Wenn Sie Ihre Einstellungen ändern oder Ihre Einwilligung jederzeit widerrufen möchten, finden Sie den Link dazu in unserer Datenschutzerklärung, die von unserer Homepage aus zugänglich ist.

[Einstellungen verwalten](#) [Weiter mit den empfohlenen Cookies](#)

Verwendungszwecke

Informationen auf einem Gerät speichern und/oder abrufen ☐ +	Auswahl einfacher Anzeigen ☒ Legitimes Interesse ☒ Zustimmung ☐ +
Ein personalisiertes Anzeigen-Profil erstellen ☒ Legitimes Interesse ☒ Zustimmung ☐ +	Personalisierte Anzeigen auswählen ☒ Legitimes Interesse ☒ Zustimmung ☐ +
Ein personalisiertes Inhalts-Profil erstellen ☒ Legitimes Interesse ☒ Zustimmung ☐ +	Personalisierte Inhalte auswählen ☒ Legitimes Interesse ☒ Zustimmung ☐ +

[Anbieter-Liste](#) [Einstellungen speichern & Beenden](#) [Weiter mit den empfohlenen Cookies](#)

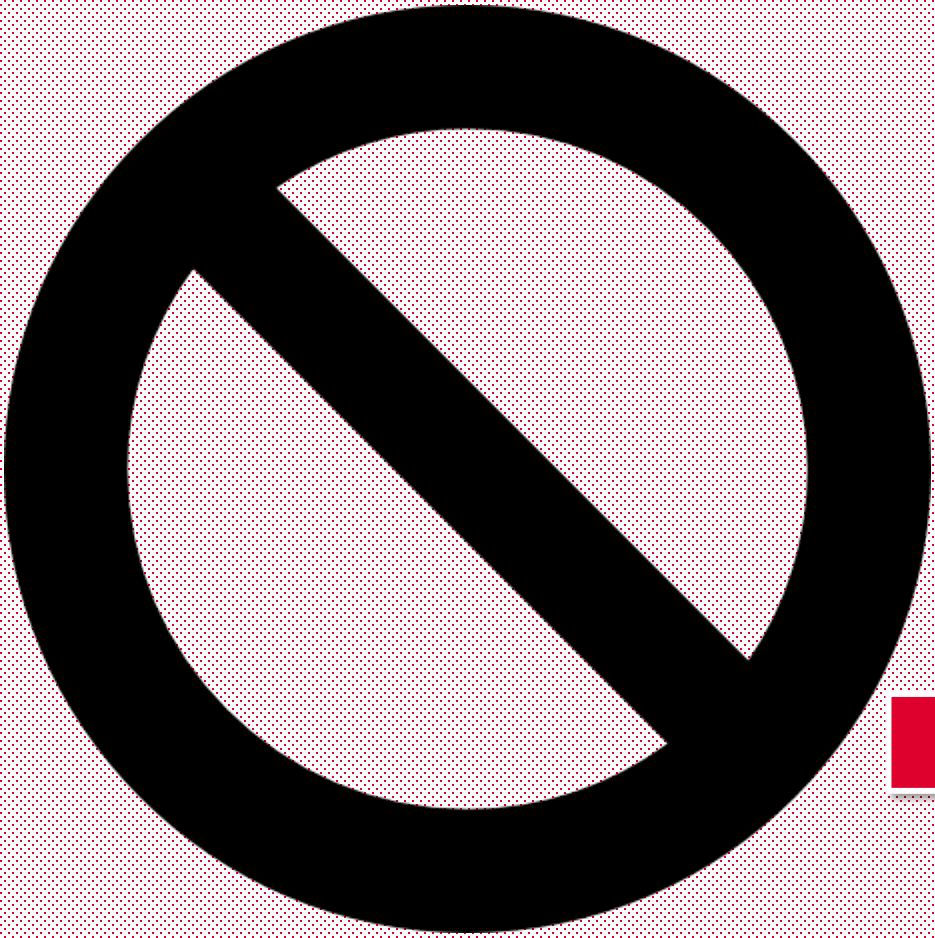
Anbieter-Liste

Exponential Interactive, Inc d/b/a VDX.tv ☐ Zustimmung ☐ +	Captify Technologies Limited ☐ Zustimmung ☐ +
Roqad GmbH ☐ Zustimmung ☐ +	Adspirit GmbH ☐ Zustimmung ☐ +
Emerse Sverige AB ☒ Legitimes Interesse ☒ Zustimmung ☐ +	Index Exchange Inc. ☐ Zustimmung ☐ +

[Einstellungen verwalten](#) [Einstellungen speichern & Beenden](#) [Weiter mit den empfohlenen Cookies](#)

Konsequenzen

- Es entstehen Vorurteile.
- Es entstehen negative Erlebnisse.
- Es entsteht Unverständnis.
- Es entsteht das Gefühl der Bevormundung.



Datenschutz wird einseitig
negativ wahrgenommen!

Ursachen der negativen Wahrnehmung

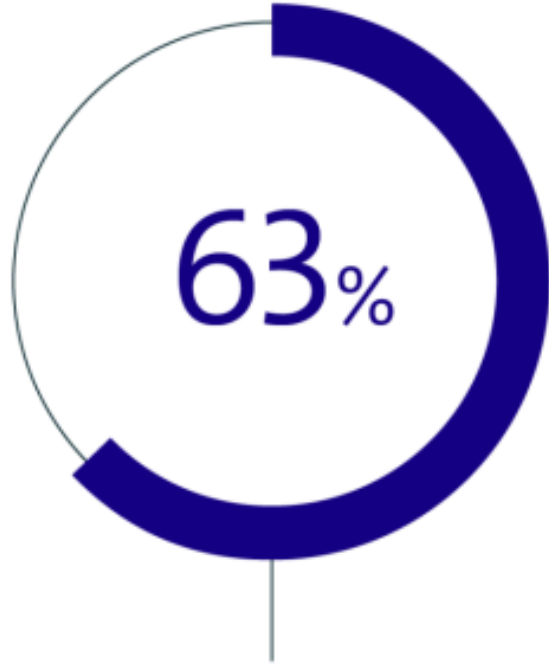
- Datenschutz wird als Ausrede verwendet
- Datenschutz wird missverstanden
- Datenschutz wird mit Datensicherheit verwechselt



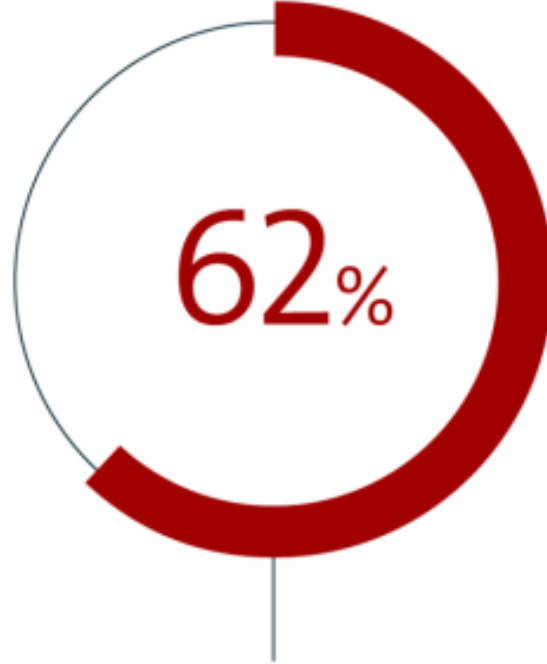
Die Betroffenen wissen zwar um ihre Rechte,
kennen aber nicht die (rechtlichen)
Hintergründe

Regeln zur Datennutzung schränken Unternehmen ein

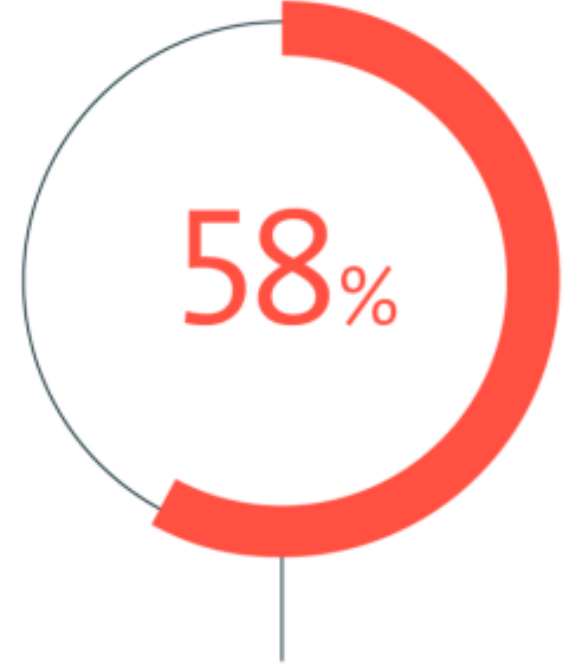
Inwieweit stimmen Sie den folgenden Aussagen zu bzw. nicht zu?



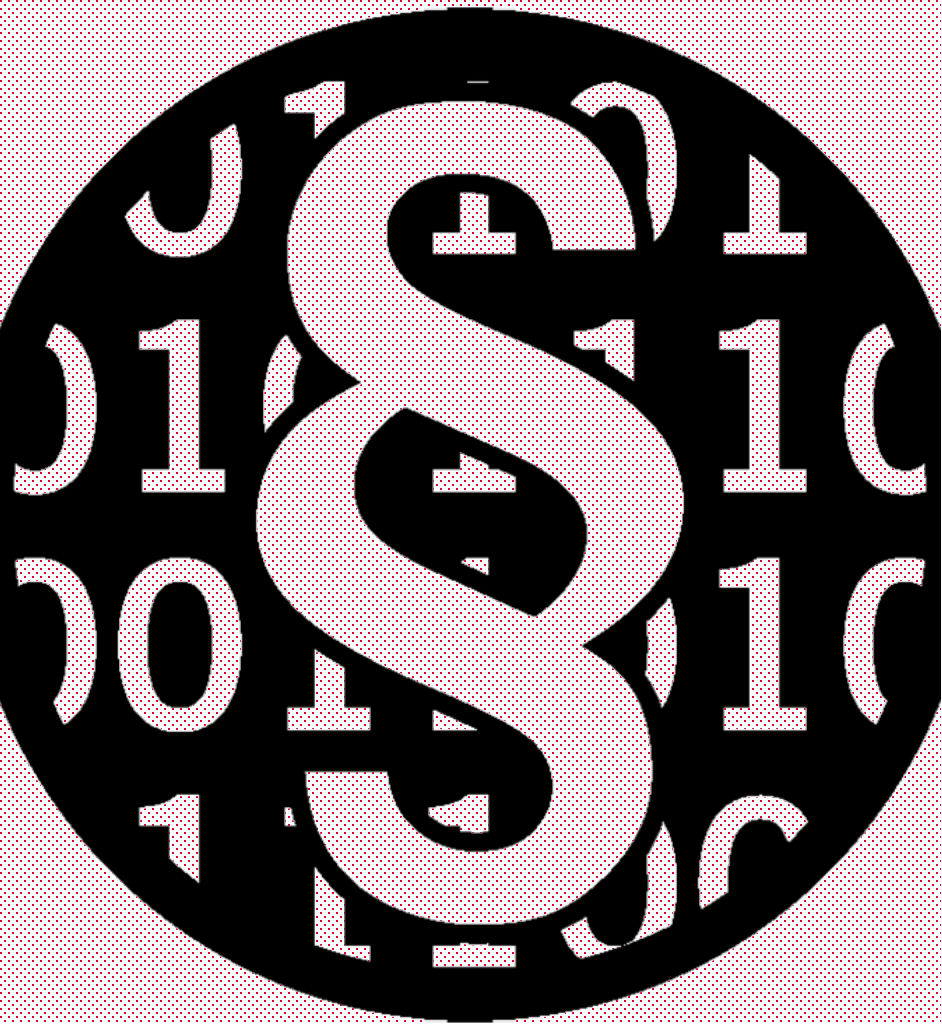
Durch strenge Regeln werden **innovative datengetriebene Geschäftsmodelle** in Deutschland erstickt oder aus dem Land vertrieben.



Wir zögern bei der Datennutzung, weil wir **Angst haben**, gegen den Datenschutz zu verstoßen.



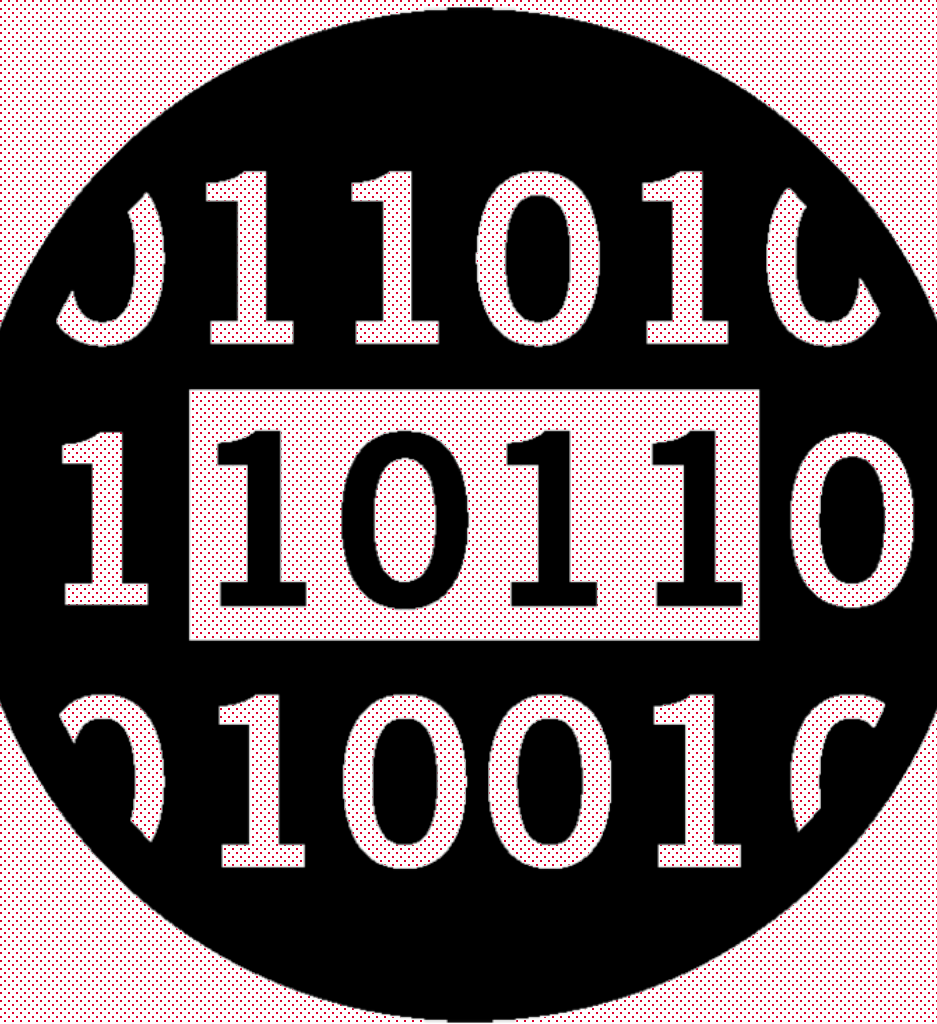
Deutschland **verschenkt Chancen** für Wachstum und Wohlstand, weil zu oft auf Datennutzung verzichtet wird.



Rechtsgrundlagen: Innovative Datenverarbeitungen

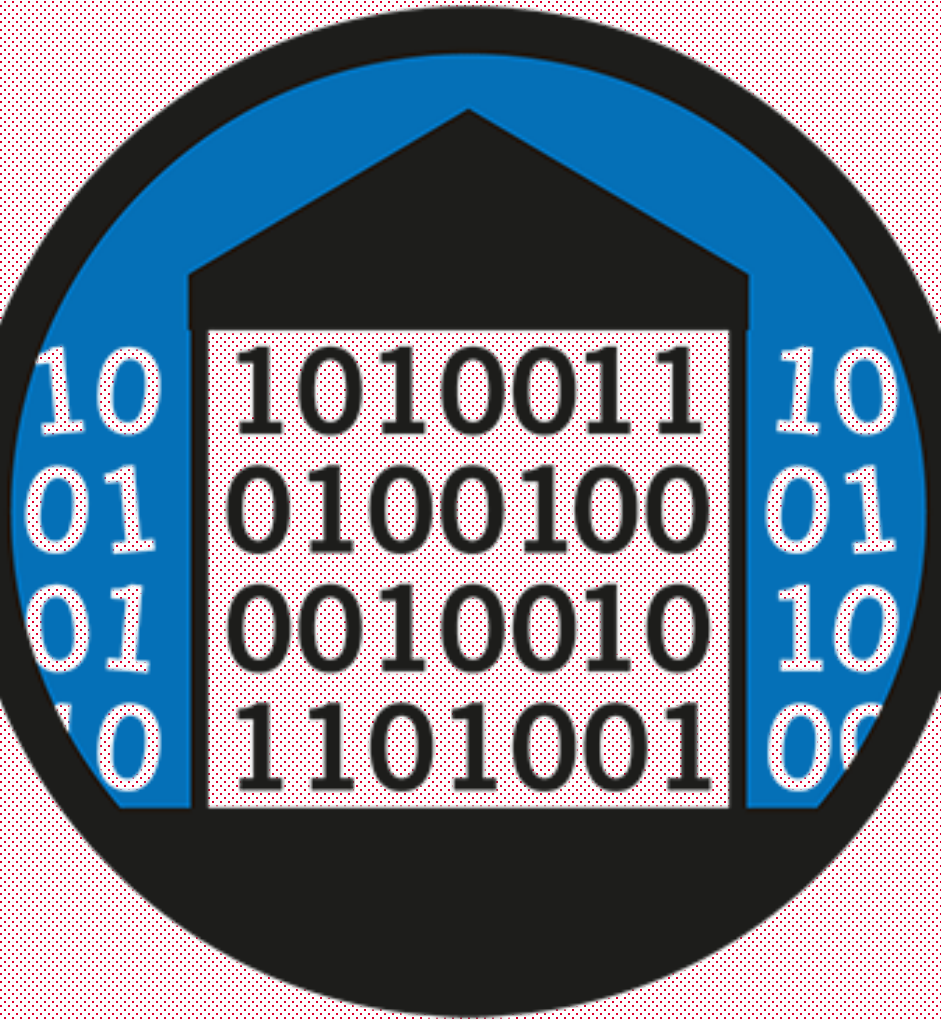
- Art. 5 DSGVO: Datenschutz-Grundsätze
- Art. 6 Abs. 1 DSGVO: Verbot mit Erlaubnisvorbehalt
- Art. 35 DSGVO: Datenschutz-Folgenabschätzung erforderlich

Aus der Praxis: Einführung von MS 365



Bewertung der „Microsoft-Onlinedienste“ durch die DSK

Datenschutzbehörden erklären den Einsatz von
Microsoft 365 für rechtswidrig



Die Aufsichtsbehörden

- Aufsichtsbehörden: Art. 51. ff. DSGVO
- Aufgaben und Befugnisse: Art. 57 und 58 DSGVO:
 - ✓ Überwachung und Durchsetzung der DSGVO
 - ✓ Sensibilisierung von Verantwortlichen und Auftragsverarbeitern
 - ~~✓ § 38 Abs. 1 BDSG a.F.: Beratungsfunktion~~
 - ✓ Art. 58 Abs. 1 lit. d) DSGVO: Beratung durch die Hintertür



Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK)

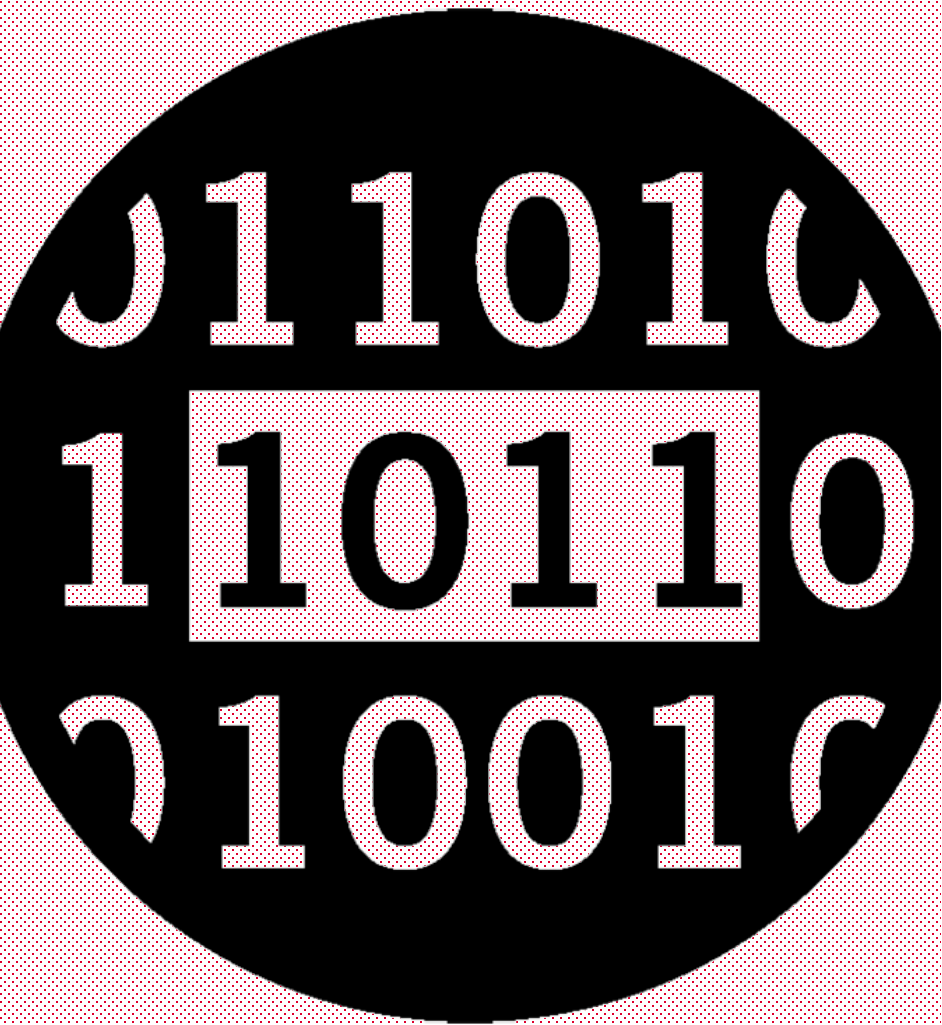
Über die Datenschutzkonferenz (DSK)

Die Datenschutzkonferenz besteht aus den unabhängigen Datenschutzbehörden des Bundes und der Länder. Sie hat die Aufgabe, die Datenschutzgrundrechte zu wahren und zu schützen, eine einheitliche Anwendung des europäischen und nationalen Datenschutzrechts zu erreichen und gemeinsam für seine Fortentwicklung einzutreten. Dies geschieht namentlich durch Entschlüsse, Beschlüsse, Orientierungshilfen, Standardisierungen, Stellungnahmen, Pressemitteilungen und Festlegungen.

[Geschäftsordnung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder \(DSK\)](#)



Rechtsunsicherheit



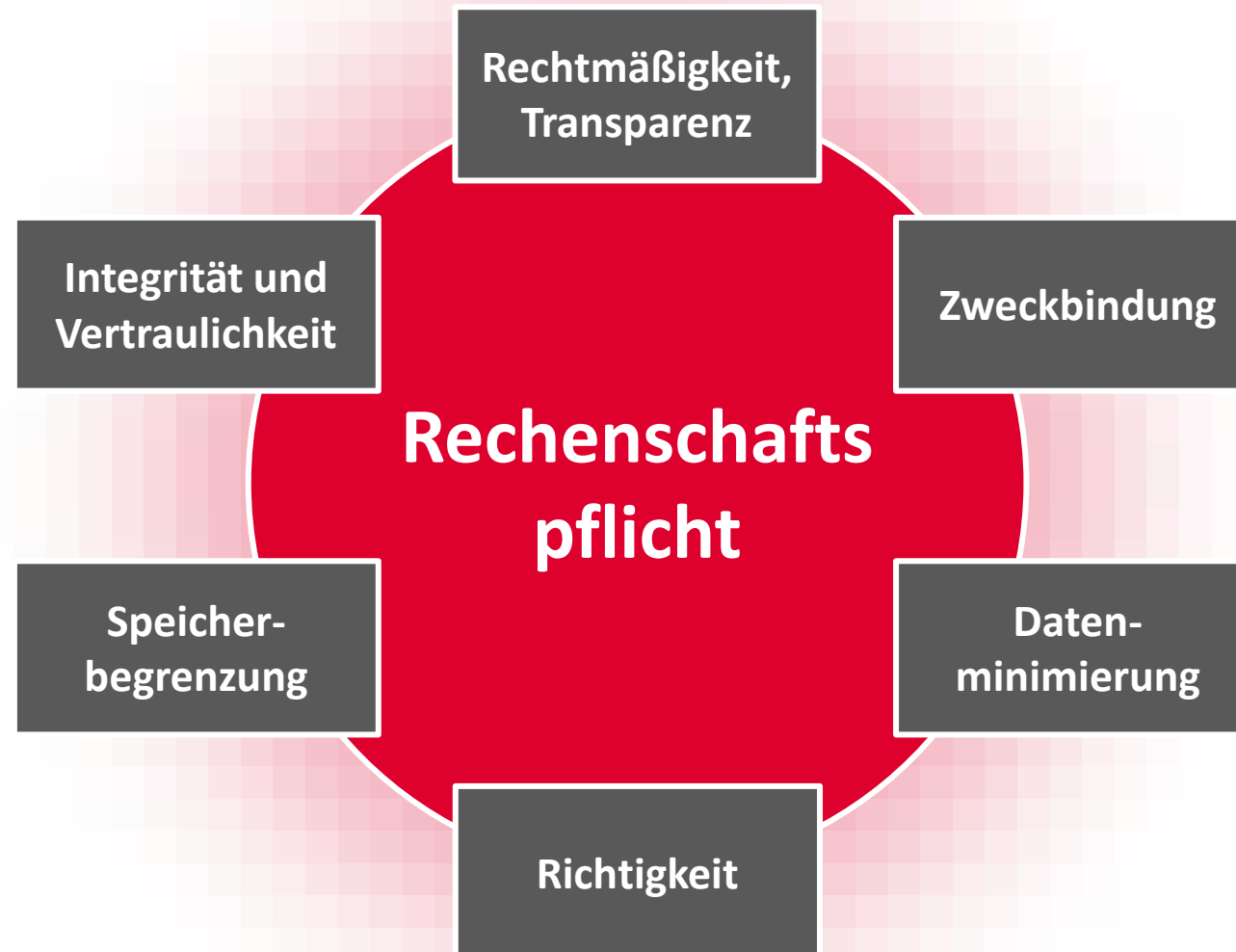
Aus der Praxis: Einführung von MS 365

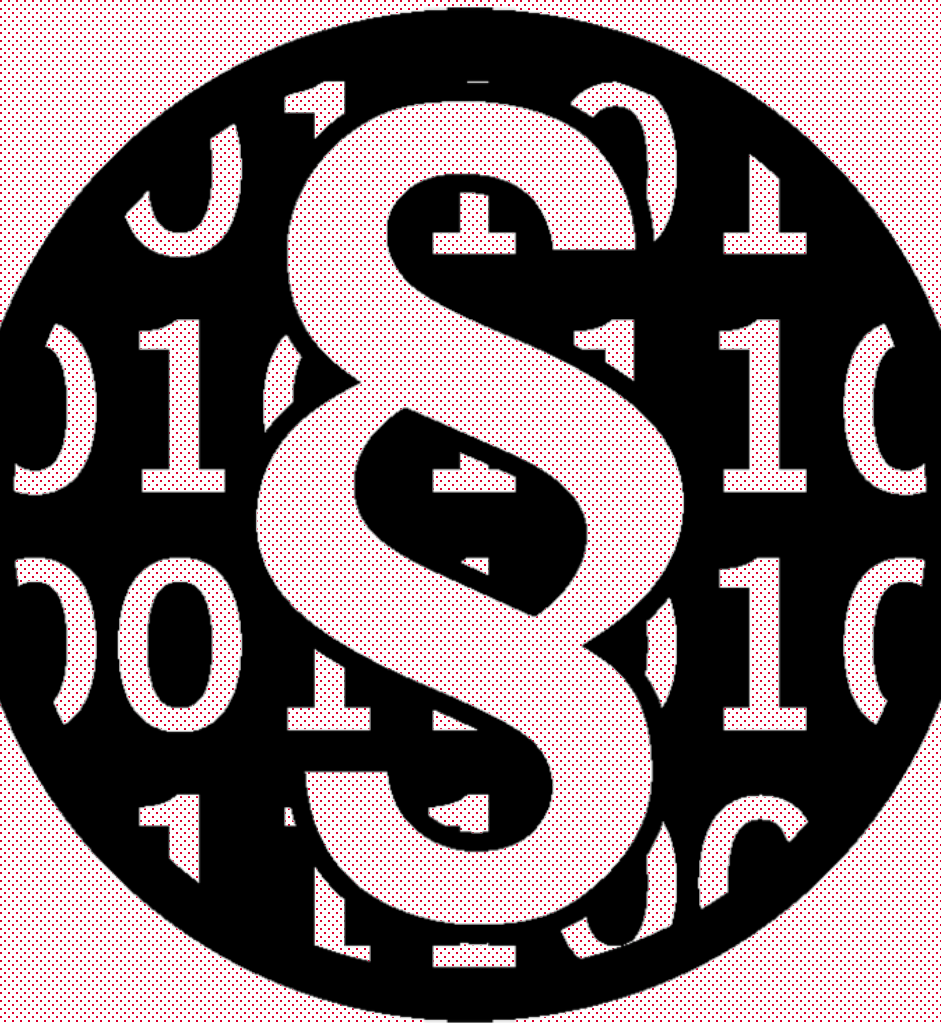
Datenschutzbehörden erklären den Einsatz von Microsoft 365 für rechtswidrig

(Kein) Verbot durch die DSGVO?

Es kommt darauf an!

Datenschutzgrundsätze





Rechtsgrundlagen

- Art. 6 Abs.1 lit. f) DSGVO: berechtigtes Interesse
- Art. 28 DSGVO: Auftragsverarbeitung
- Art. 44 ff. DSGVO: Datenübermittlung in Drittstaaten
- Art. 35 DSGVO: Risikoabschätzung

Problem: Auslegung der Rechtsgrundlagen durch die Aufsichtsbehörden, unterschiedliche Beurteilung der Risiken für die betroffenen Personen durch Verantwortliche, Auftragsverarbeiter und Aufsichtsbehörden

Clouddienste und Datenschutz nach der DSGVO

- Ank
- Auf
- Abg
- Um
- Kei

Amazon Web Services startet AWS European Sovereign Cloud

- Die AWS European Sovereign Cloud wird eine neue, unabhängige Cloud für Europa sein. Kunden aus stark regulierten Industrien und dem öffentlichen Sektor erhalten damit mehr Auswahl und Flexibilität, um den steigenden Anforderungen an den Ort der Datenverarbeitung und die operative Souveränität in der Europäischen Union (EU) besser gerecht zu werden
- Für Kunden der AWS European Sovereign Cloud wird es möglich sein, alle von ihnen erstellten Metadaten in der EU zu belassen
- Die Kontrolle über den Betrieb und den Support der AWS European Sovereign Cloud wird ausschließlich von AWS-Personal ausgeübt, das in der EU ansässig ist und sich in der EU aufhält
- Aufsichtsbehörden wie das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI), das deutsche Bundesministerium des Innern und für Heimat (BMI) und das deutsche Bundesministerium für Digitales und Verkehr (BMDV), das finnische Finanzministerium, die tschechische Nationale Agentur für Cyber- und Informationssicherheit (NÚKIB), das rumänische Kompetenzzentrum für Cybersicherheit, sowie AWS-Kunden und -Partner, wie SAP, Dedalus, Deutsche Telekom, O2 Telefónica Deutschland, Heidelberger Druckmaschinen AG, Raisin, Scalable Capital, de Volksbank, Telia Company, Accenture, Almayviva, Deloitte, Eviden, Materna und msg-Gruppe, begrüßen die Einführung der AWS European Sovereign Cloud

25.10.2023 | Berlin

Amazon Web Services (AWS) kündigte heute den zukünftigen Start der AWS European Sovereign Cloud an. Die neue unabhängige Cloud für Europa soll Kunden aus dem öffentlichen Sektor und stark regulierten Industrien – zum Beispiel Betreiber kritischer Infrastrukturen („KRITIS“) – dabei helfen, spezifische gesetzliche Anforderungen an den Ort der Datenverarbeitung und an den Betrieb der Cloud zu erfüllen. Die AWS European Sovereign Cloud wird sich in der EU befinden und dort betrieben. Sie wird physisch und logisch von den bestehenden AWS-Regionen getrennt sein und dieselbe Sicherheit, Verfügbarkeit und Leistung wie die bestehenden AWS-Regionen bieten. Damit haben Kunden eine zusätzliche Wahlmöglichkeit, um Anforderungen an den Ort der Datenverarbeitung, die betriebliche Autonomie und die operative Souveränität zu erfüllen. Die AWS European Sovereign Cloud wird mit ihrer

isch

diagnoseda

Microsoft announces the phased rollout of the EU Data Boundary for the Microsoft Cloud begins January 1, 2023

Dec 15, 2022 | Julie Brill, Corporate Vice President and Chief Privacy Officer, Privacy and Regulatory Affairs, and Erin Chapple, Corporate Vice President, Azure Core Product and Design

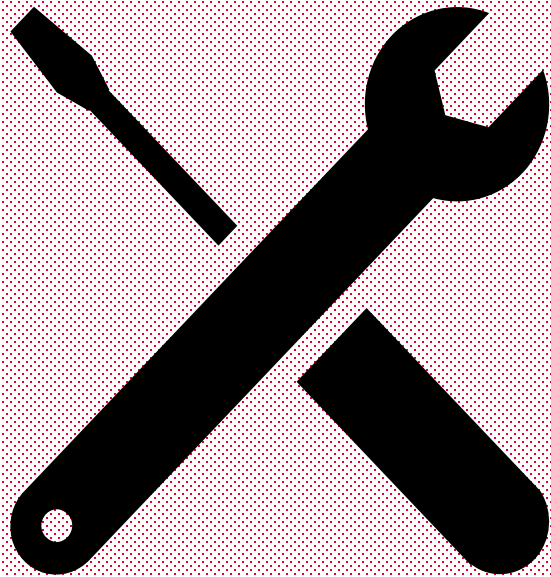


In today's global economy, commercial and public sector customers continue to look for ways to advance their goals, protect their data and scale for improved efficiencies. To support these changing requirements, Microsoft is committed to providing trusted cloud services that are designed to take advantage of the full power of the public cloud while respecting European values and sovereignty needs.

Today, we are announcing that, on January 1, 2023, Microsoft will begin a phased rollout of our EU Data Boundary solution to public sector and commercial customers in the European Union (EU) and the European Free Trade Association (EFTA).

Microsoft's on-going commitment to Europe

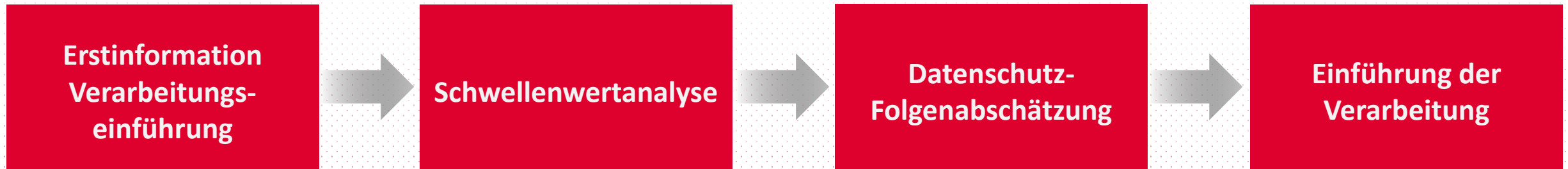
Microsoft remains deeply committed to supporting European digital needs and has adopted five [European Cloud Principles](#) that guide our cloud business across Europe. Microsoft offers data residency and proximity in



Auf die Umsetzung kommt es an!

- W-Fragen stellen
- Fahrplan aufstellen
- Konzept: Einführung von neuen Verarbeitungen
- Schwellenwert-Analyse/ Risikobewertung
- Datenschutz-Folgenabschätzung
- Technische und Organisatorische Maßnahmen
- Zusammenarbeit mit der Aufsichtsbehörde

Rechtskonforme Einführung neuer Datenverarbeitung





W-Fragen

- Warum soll eine Technologie/ Verarbeitung eingeführt werden (Rechtmäßigkeit/ Transparenz/ Notwendigkeit)?
- Welche Zwecke werden damit verfolgt (Zweckbindungsgrundsatz)?
- Welche Mengen an Daten müssen verarbeitet werden (Datenminimierung)?
- Wer wird davon berührt/ wer sind die Betroffenen (Transparenz/ Integrität/ Vertraulichkeit) ?
- Welcher Zeitraum steht mir zur Verfügung ?



Risiko nach DSGVO (1)

- Risikobegriff:

Hinsichtlich Eintrittswahrscheinlichkeit und Schwere zu bestimmendes Risiko für die Rechte und Freiheiten natürlicher Personen.

- Risikobestimmung:

„Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Person sollten in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung bestimmt werden.“ (ErwGr 76)



Risiko nach DSGVO (2)

Regelungen mit Risikobezug:

- Pflicht zur Führung des Verzeichnisses der Verarbeitungstätigkeiten (Art. 30 DSGVO)
- Zu ergreifende TOMs (Art. 24, 32 DSGVO)
- Pflicht zur Meldung eines Vorfalls (Art. 33 DSGVO)

Regelungen bei hohem Risiko:

- Pflicht zur Betroffeneninformation (Art. 43 DSGVO)
- Durchführung einer DSFA (Art. 35 DSGVO)

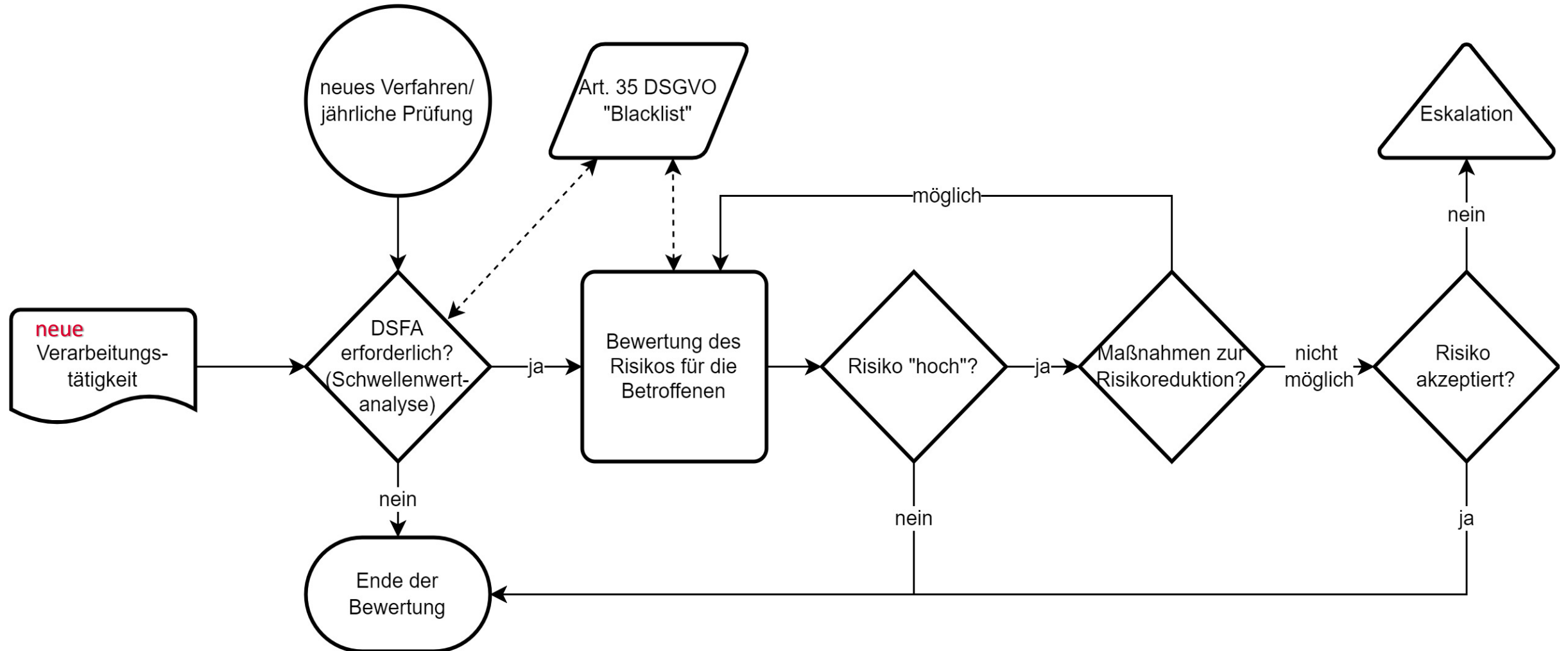


Risiko nach DSGVO (3)

Datenschutzfolgenabschätzung (DSFA, Art. 35 Abs. 7 DSGVO):

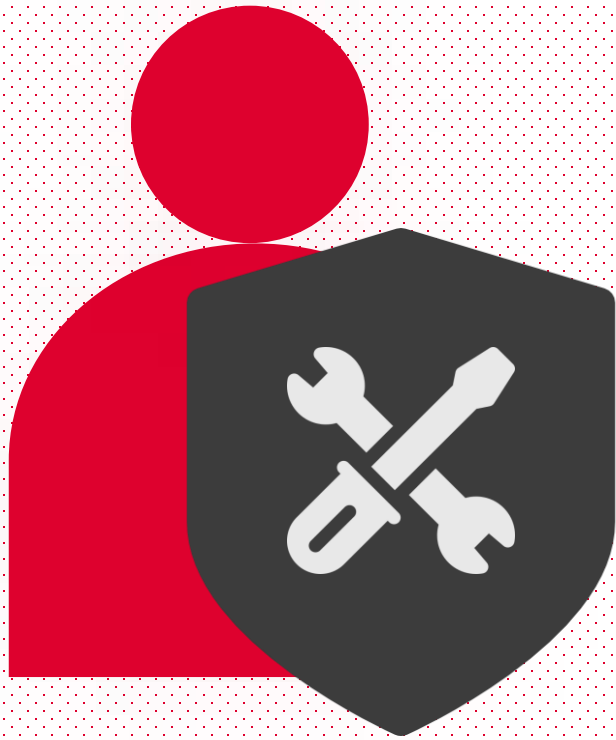
- Systematische Beschreibung der Verarbeitungsvorgänge, Zwecke und berechtigten Interessen
- Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitung in Bezug zum Zweck
- Bewertung des potentiellen Risikos für Betroffene
- Abhilfemaßnahmen zur Bewältigung der Risiken (Garantien, Sicherheitsvorkehrungen, Verfahren)

Prozess der Risikobewertung (DSFA)



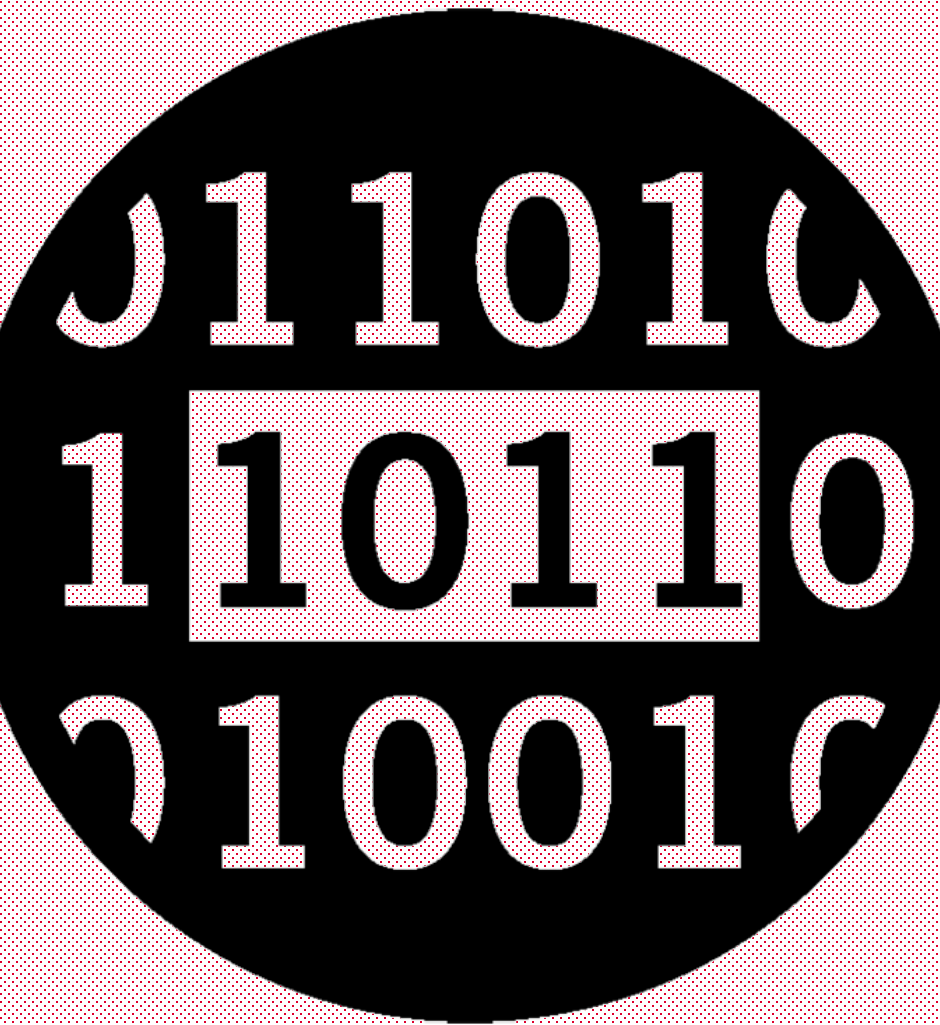
Technische Schutzmaßnahmen

Clouddienste



- Art. 32 DSGVO: Sicherheit der Verarbeitung (Integrität und Vertraulichkeit)
- DSGVO ist technikneutral
- Hinweise BSI: Sichere Einführung von Clouddiensten; IT-Grundschutz-Kompendium
- Hinweise LDA Bayern: Good Practice bei technischen und organisatorischen Maßnahmen

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Sichere_Nutzung_Cloud_Dienste.pdf?__blob=publicationFile&v=10; http://www.lida.bayern.de/media/checkliste/baylda_checkliste_tom.pdf



Aus der Praxis: Einführung von MS 365

- ✓ Rechtsgrundlagen
 - ✓ Auftragsverarbeitungsvertrag
 - ✓ DSFA
 - ✓ Umsetzung der Maßnahmen aus der DSFA
 - ✓ Beachtung PDCA-Zyklus
- Einführung und Nutzung ist möglich!



Datenverarbeitung in der Forschung

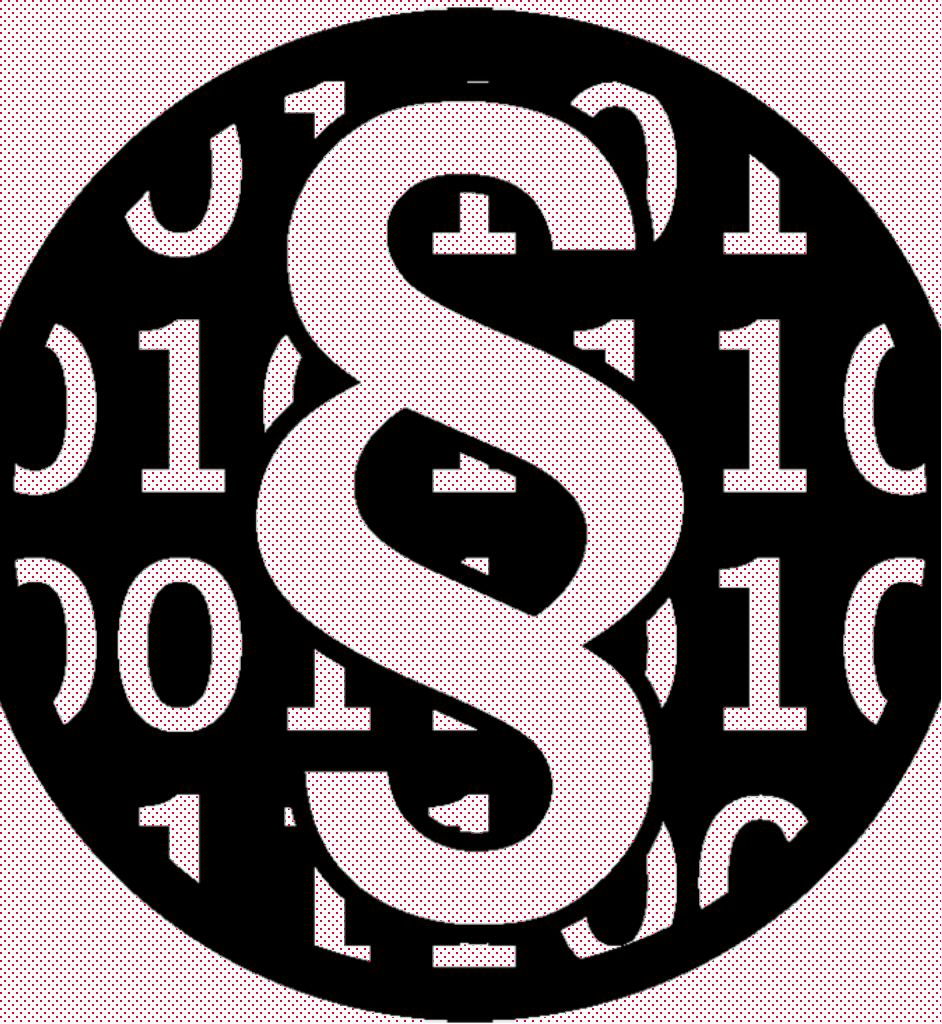
„Die Kombination unseres strikten Datenschutzes mit der wenig pragmatischen Kultur der Datennutzung kostet Leben“



Alena Buyx, Jahrgang 1977, studierte Medizin, Philosophie, Soziologie und Gesundheitswissenschaften. Seit 2020 ist sie Vorsitzende des Deutschen Ethikrats. (Foto: Political Moments/Jutta Prechtel/SZ Photo)

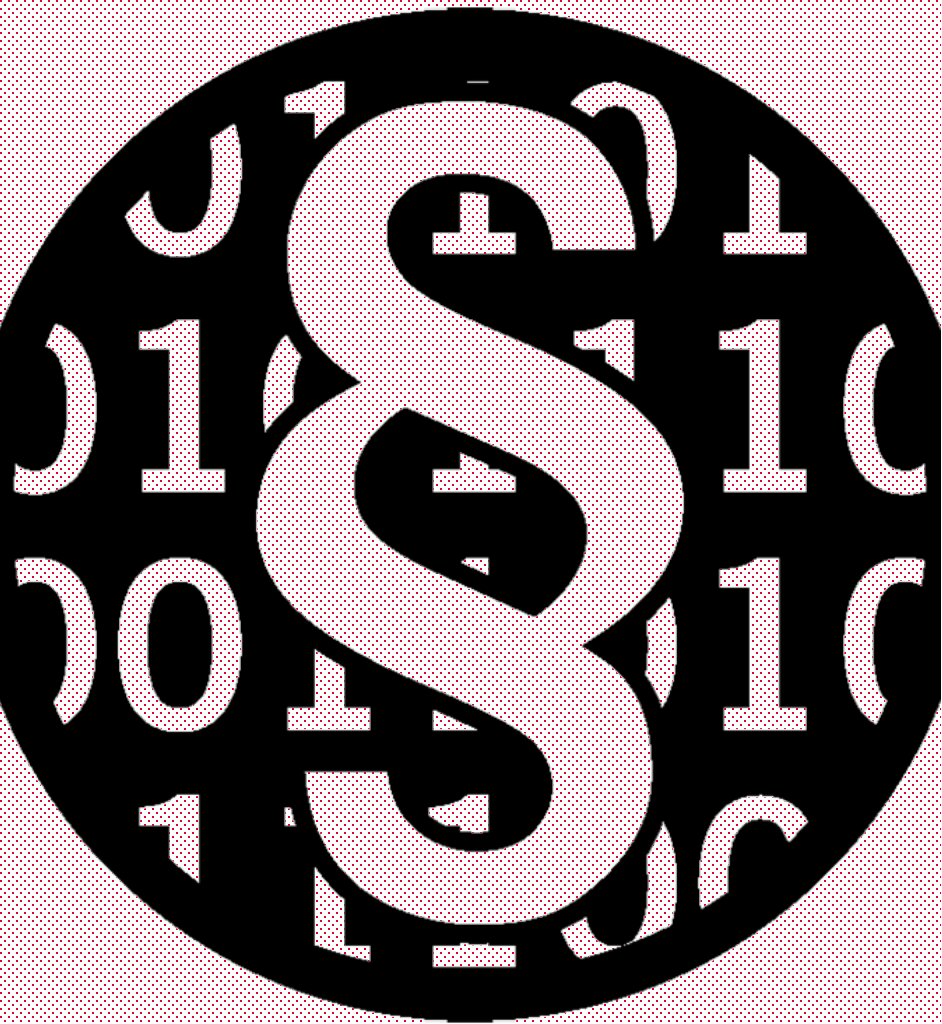
Deutschland sollte sich eher auf die Chancen als auf die Risiken der Digitalisierung im Gesundheitswesen fokussieren, findet die Ethikratsvorsitzende Alena Buyx. Ab wann Datenschutz den Patienten schadet – und wie sie es in Zukunft einfacher haben könnten.

<https://www.sueddeutsche.de/wissen/datenschutz-gesundheitswesen-e-rezept-elektronische-patientenakte-digitalisierung-ethik-1.5711682>



Rechtsgrundlagen Forschung I

- § 27 BDSG:
 - Keine Einwilligung bei besonderen personenbezogenen Daten bei wissenschaftlichen oder historischen Forschungszwecken und statistischen Zwecken erforderlich
 - Einschränkung der Betroffenenrechte
 - Pflicht zur Anonymisierung
 - Veröffentlichung nur mit Einwilligung
- Art. 5 Abs. 1 lit. b) DSGVO: Forschungsprivileg: Weiterverarbeitung
- Art. 89 DSGVO: Garantien und Ausnahmen



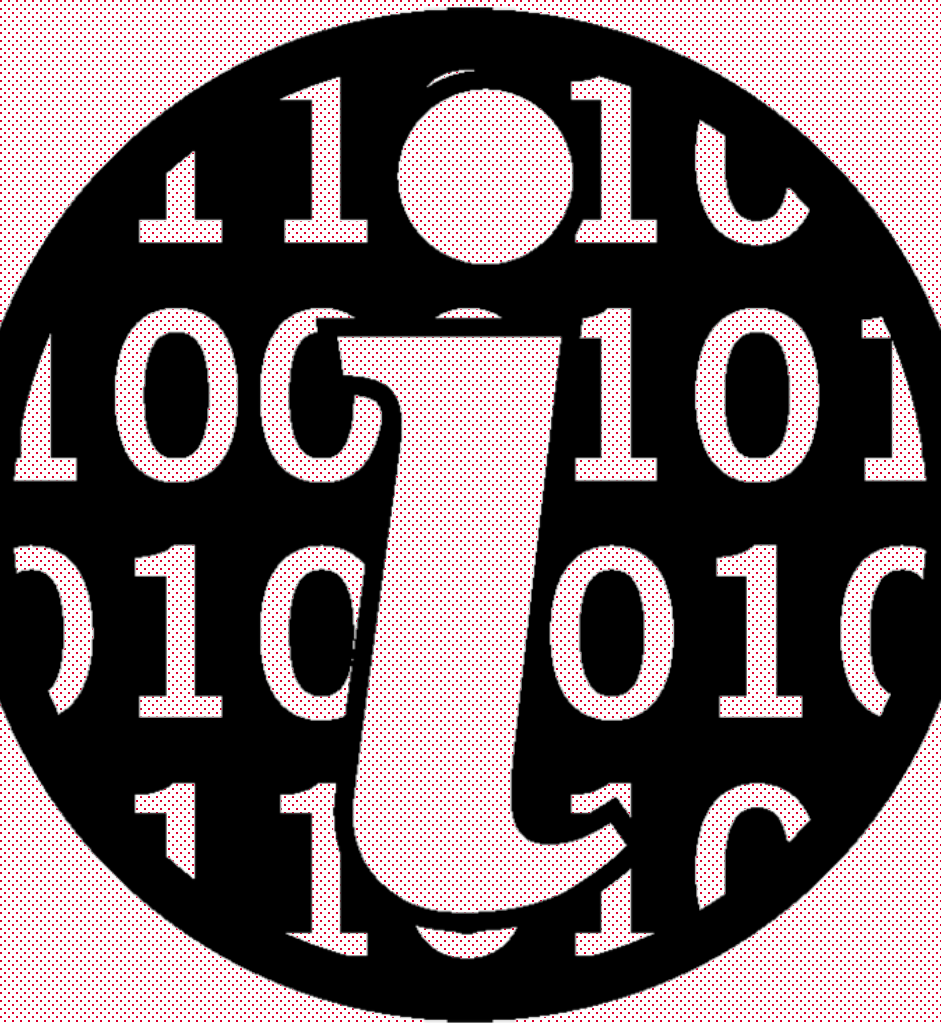
Rechtsgrundlagen Forschung II

- Art. 5 Abs. 1 lit. b) DSGVO: Forschungsprivileg: Weiterverarbeitung:
 - Ausnahme vom Zweckbindungsgrundsatz
- Art. 89 DSGVO: Garantien und Ausnahmen:
 - Garantien und Maßnahmen zur Gewährleistung des Grundsatzes der Datenminimierung
 - Ausnahmen bei den Betroffenenrechten

Recht anpassen

In Deutschland liegen Gesundheitsdaten derzeit jedoch nicht in ausreichendem Maß für eine Weiternutzung außerhalb des unmittelbaren Versorgungskontextes vor beziehungsweise werden nicht ausreichend genutzt. Eine Weiternutzung scheitert aktuell häufig an unterschiedlichen Regelungen bzgl. des Zugangs zu Daten und bzgl. des Datenschutzes im Europäischen Recht Bundes-, Landesrecht sowie an einer uneinheitlichen Rechtsauslegung durch Datenschutzbeauftragte und Aufsichtsbehörden. Fehlende Vorgaben und Verfahren zur Verknüpfung von Daten aus unterschiedlichen Quellen stellen eine weitere Hürde für die Datennutzung dar.

Durch diese Rechtsunsicherheit werden Forschung und Innovation gehemmt; die Potentiale der Datennutzung in unserem Gesundheitswesen bleiben ungenutzt. Forschende und andere Akteure, die Gesundheitsdaten im Sinne des Gemeinwohls verarbeiten wollen, stoßen daher vielfach auf Hemmnisse bei dem Versuch für ihre Aufgaben und Forschungsvorhaben Zugang zu den erforderlichen Daten zu erhalten.



Abhilfe Forschung

- Bessere Informationen für Forschende
- Beratung durch die Aufsichtsbehörden verbessern
- Klarere gesetzliche Regelungen



Was sonst noch hilft...

- Information der Betroffenen und Verantwortlichen und Auftragsverarbeiter
- Frühzeitige Vermittlung der Datenschutzgrundlagen:



Und jetzt?

Datenschutz – nur in der EU?

Bottom 5 non-EU countries

1. China – 1.8 – Extensive surveillance
2. Russia – 2.1 – Systemic failure to maintain safeguards
3. India – 2.4 – Systemic failure to maintain safeguards
4. Thailand – 2.6 – Some safeguards but weakened protections
5. Malaysia – 2.6 – Some safeguards but weakened protections

Non-EU Surveillance Societies

Scoring system (for each category and overall)

4.1-5.0 = Upholding privacy standards on a consistent basis

3.6-4.0 = Significant safeguards and protections

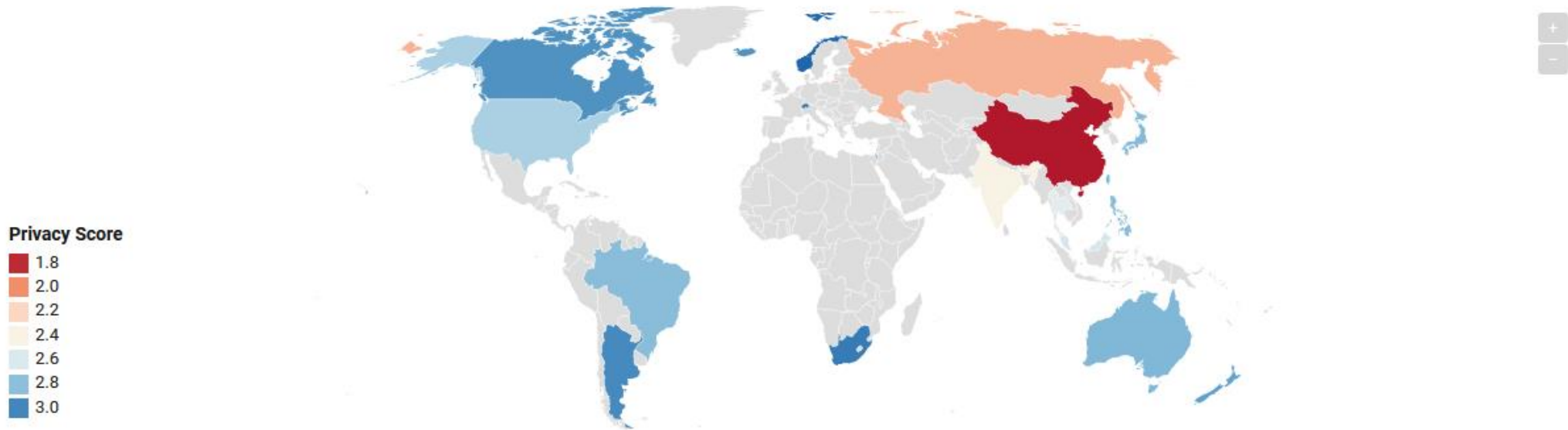
3.1-3.5 = Adequate safeguards against abuse

2.6-3.0 = Some safeguards but weakened protections

2.1-2.5 = Systemic failure to maintain safeguards

1.6-2.0 = Extensive surveillance

1.1-1.5 = Endemic surveillance



Datenschutzniveau innerhalb der EU

Bottom 5 EU countries

1. Italy – 2.7 – Some Safeguards/Weakened Protection
2. Hungary – 2.7 – Some Safeguards/Weakened Protection
3. Slovenia – 2.7 – Some Safeguards/Weakened Protection
4. Germany – 2.8 – Some Safeguards/Weakened Protection
5. Spain – 2.9 – Some Safeguards/Weakened Protection

EU Surveillance Societies

Germany

Despite privacy enforcement in a number of areas (sensitive data and the implementation of the data protection law, Bundesdatenschutzgesetz) and the active role of its Data Protection Conference, Germany is failing its citizens in a number of areas. These include:

- Its extensive use of biometrics, including in a national ID card
- Being a founding member of the Treaty of Prüm and Schengen Agreement
- Its allowance of CCTV cameras with facial recognition
- Controversial data retention directives
- Lack of privacy protection for journalists
- Heavy censorship of social media posts through "hate speech" laws



Datenschutzniveau innerhalb der EU

Top 5 EU countries

Due to the recent implementation of the GDPR laws, there isn't much difference in the scores of EU countries. What tends to differentiate them is their data-sharing agreements with other countries, their freedom of speech, their use of biometrics, and other country-specific rules and regulations.

1. Ireland – 3.2 – Adequate Safeguards
2. France – 3.1 – Adequate Safeguards
3. Portugal – 3.1 – Adequate Safeguards

Irland plant Gesetzesänderung

Maulkorb bei Datenschutz-Verstößen

Die irische Datenschutz-Aufsichtsbehörde soll Verfahren als „vertraulich“ einstufen dürfen. Das würde auch Fälle gegen Big-Tech-Konzerne betreffen.

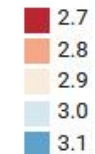
privacy (18 ongoing investigations into US

- Its resistance toward biometrics on ID cards, despite it being an EU regulation
- It not being part of invasive data-sharing agreements, i.e. the Treaty of Prüm or the Schengen Agreement
- An active role in overturning the EU's data retention directive due to its breach of privacy and human rights
- Its opt-out clause for EU laws

The categories that let Ireland down were its weakened protections for sensitive data (i.e. several data breaches in the medical industry), the subsidization of CCTV, and a threat to press freedom due to the concentrated ownership of media outlets.



Privacy Score



Machtwort des EDPB

EDPB adopts Art. 65 dispute resolution binding decisions regarding Facebook, Instagram and WhatsApp

📅 6 December 2022 **EDPB**

Brussels, 6 December - The EDPB adopted three **dispute resolution decisions on the basis of Art. 65 GDPR concerning Meta Platforms Ireland Limited** (Meta IE). The binding decisions address important legal issues arising from the draft decisions of the Irish SA as lead supervisory authority (LSA) regarding Meta IE platforms Facebook, Instagram and WhatsApp. The EDPB binding decisions play a key role in ensuring the correct and consistent application of the GDPR by the national Supervisory Authorities.

The Irish SA issued the draft decisions following complaint-based inquiries into the processing activities of the three platforms. The Facebook and Instagram draft decisions concern, in particular, the lawfulness and transparency of processing for behavioural advertising. The WhatsApp draft decision concerns notably the lawfulness of processing for the purpose of the improvement of services. Several SAs issued objections on the draft decisions prepared by the Irish SA concerning, among others, the legal basis for processing (Art. 6 GDPR), data protection principles (Art. 5 GDPR), and the use of corrective measures including fines.

As no consensus was reached on these objections, the EDPB was called upon to settle the dispute between the SAs within two months.

In its binding decisions, **the EDPB settles, among others, the question of whether or not the processing of personal data for the performance of a contract is a suitable legal basis for behavioural advertising, in the cases of Facebook and Instagram, and for service improvement, in the case of WhatsApp.**

The LSA shall adopt its three final decisions, addressed to the controller, on the basis of the EDPB binding decisions, taking into account the EDPB's legal assessment, at the latest one month after the EDPB has notified its decisions. The EDPB will publish its decisions on its website after the LSA has notified its national decisions to the controller.



Latest news

Croatian SA imposed an administrative fine on the Debt Collector – the Debt Collecting Agency – amount of 5.470.000,00 EUR 9, 12, 13 and 32 of the GDPR

📅 5 October 2023 **Croatia**

September plenary - adopted

📅 4 October 2023 **EDPB**

EDPB adopts Guidelines on data protection by design and by default appropriate safeguards under

📅 27 September 2023 **EDPB**

Swift adoption of Regulation 1734/2023 on enforcement needed

📅 21 September 2023 **EDPB**

Machtwort der Kommission

Pressemitteilung | 4. Juli 2023 | Brüssel

**Datenschutz: Kommission erlässt neue Vorschriften für
bessere Durchsetzung der DSGVO in
grenzüberschreitenden Fällen**

Wettbewerbsvorteil: Vertrauen durch Datenschutz

Datenschutz / Datensicherheit / IT / Verbraucher / Verbrauchervertrauen

Vertrauen: Datenschutz als Wettbewerbsvorteil

Unternehmen müssen aufhören, Datenschutzprogramme als Projekte zu behandeln, die nicht auf das Ergebnis einzahlen. Denn: Robuste Praktiken sorgen für höhere Umsätze und sind ein Konkurrenzvorteil.

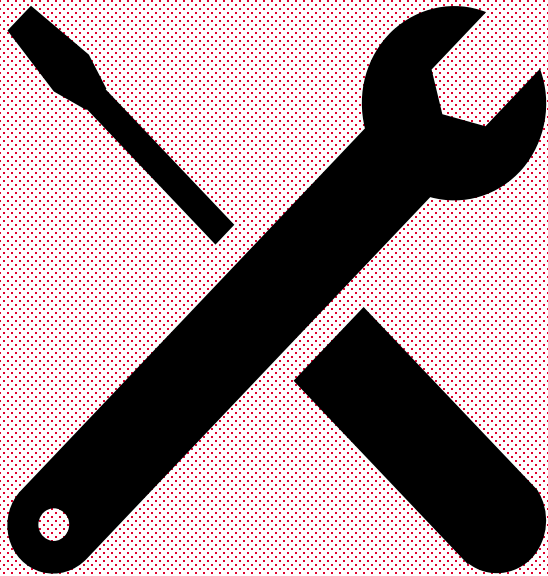
- Schadensersatzansprüche
- Imageverlust



Wettbewerbsvorteil: Vertrauen durch Datenschutz

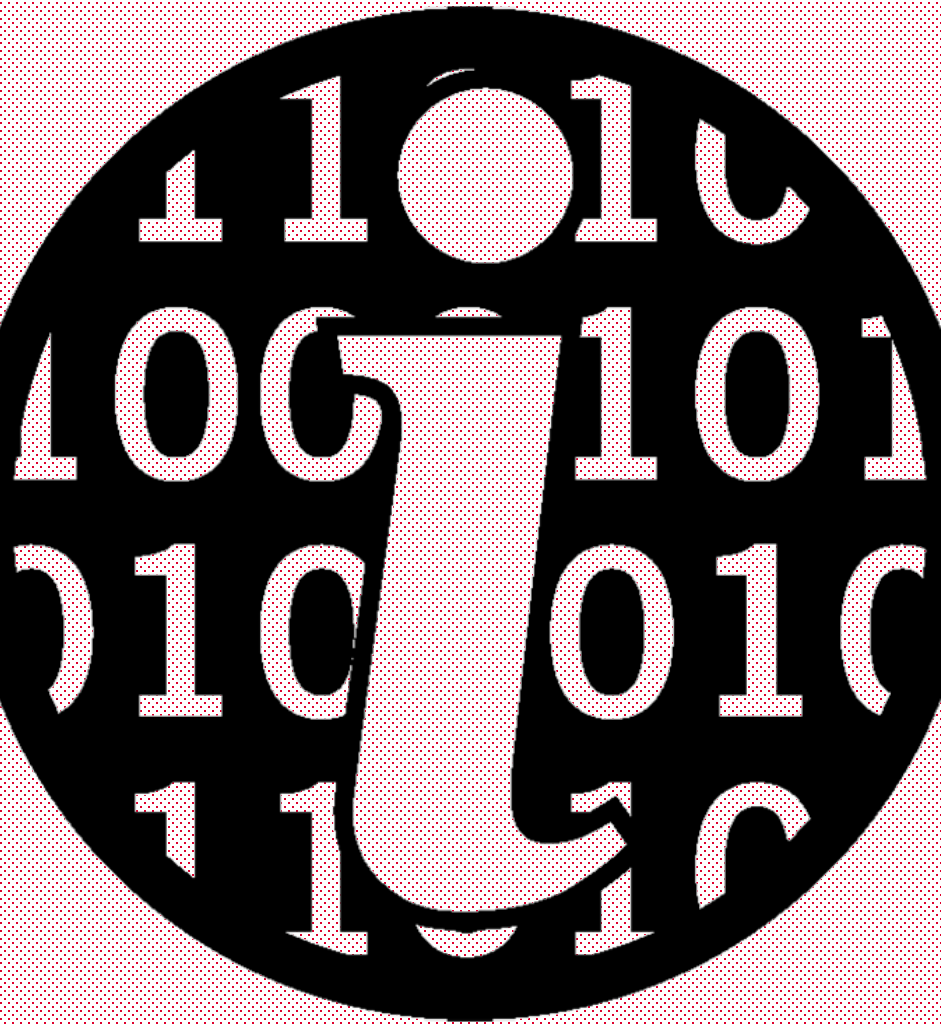
- Datenschutz als Mittel zur Wertschöpfung (added value)
- Datenschutz schafft verbesserte betriebliche Effizienz, Agilität und Innovation (data protection by design)
- Datenschutz als positives Abgrenzungsmerkmal
- Datenschutz rückt in den Verbraucherfokus

Werkzeug(e)



Datenschutzmanagement:

- Datenschutzkonzept- und Leitlinie
- Datenschutzrichtlinien
- Schulungskonzepte
- Konzepte zur Bearbeitung von Betroffenenanfragen
- Löschkonzept
- Datenschutzberichte



Datenschutzkonzept

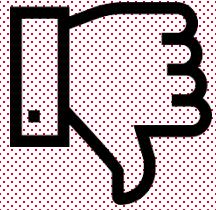
- Nachweis und Dokumentation
- Keine unmittelbare Vorgabe der DSGVO, aber u.U. Landesgesetze
- Beschreibung der nach der DSGVO erforderlichen Maßnahmen
- Dokumentation Interessenabwägung und Erforderlichkeit
- Keine Formvorgaben



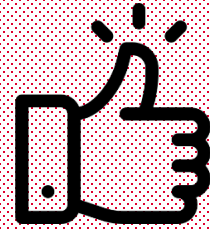
Aufbewahren und Löschen von Daten

- Aufbewahren aus Unsicherheit kostet Geld:
 - Analogen und Digitalen Speicherplatz
 - Ggfs. Bußgeld bei Verstoß gegen Art.5 Abs. 1 lit. e) DSGVO
- Daten die nicht benötigt werden dürfen nicht gespeichert werden.
- Löschkonzept spart letztlich bares Geld

Wettbewerbsvorteil oder Wettbewerbsnachteil



- Nachteile entstehen durch Vorurteile und Unkenntnis
- Rechtsunsicherheit stellt ein objektives Umsetzungshindernis für Datenschutz dar
- Gesetzgeberische Maßnahmen können die Situation ggfs. teilweise verbessern



- Datenschutzniveau innerhalb der EU ist sehr gut
- Datenschutzmaßnahmen führen zu besserer Effizienz, Wirtschaftlichkeit, Innovation
- Datenschutz sorgt für Vertrauen
- Harmonisierung der Umsetzung der DSGVO verhindert Rechtsunsicherheit

Datenschutz nervt?

Nein!



Fazit

- Wenn man vor der Welle schwimmt, kann man Zukunftspotenziale frühzeitig entdecken und Maßstäbe setzen!
- Datenschutz ist kein Sprint sondern ein Marathon – das hält man durch, wenn man gut vorbereitet ist.



secorvo
security consulting

Ettlinger Str. 12-14
76137 Karlsruhe

Telefon +49 721 255171-0
Telefax +49 721 255171-100
info@secorvo.de
www.secorvo.de

Quellenangaben

- Icons made by Freepik from www.flaticon.com
- Icons made by Flation
- Bilder Titelfolie, Agenda, etc.: Wolfram Sieber/Fotoskop.de
- Bild Schlussfolie (Visitenkarte): harmonicdesign/Bigstock.com
- Bilder Secorvo-Folie (Wir lieben was, wir tun): Platz der Grundrechte - pure-life-pictures - www.stock.adobe.com | Augenmaß - Dan Race - www.stock.adobe.com
- Folie 37: Bilder: Bundesbeauftragter für Datenschutz und Informationsfreiheit
- Folien 41: Bild google maps
- Folie 51 Bild Pixaby Urheber12019

- Piktogramme: LfDI Baden-Württemberg und Bitkom