



Die Cloud da oben...
Wunderschön...
Da muss alles gut und
sicher sein...



Cloud und Datenschutz

Insbesondere auch aus Sicht des Leistungserbringers

Dr. Bernd Schütze

4. Fachtagung „Datenschutz im Gesundheitswesen“, 2022-05-12



HEALTHCARE SOLUTIONS



Deutsche Telekom Healthcare and Security Solutions GmbH

Dr. Bernd Schütze
Senior Experte Medical Data Security

+49 (160) 9566 - 3145

Bernd.Schuetze@T-Systems.com



Studium

- Informatik (FH-Dortmund)
- Humanmedizin (Uni Düsseldorf / Uni Witten/Herdecke)
- Jura (Fern-Uni Hagen)

Ergänzende Ausbildung

- Datenschutzbeauftragter (Ulmer Akademie für Datenschutz und IT-Sicherheit)
- Datenschutz-Auditor (TüV Süd)
- Medizin-Produkte-Integrator (VDE Prüf- und Zertifizierungsinstitut)

Berufserfahrung

- Über 10 Jahre klinische Erfahrung
- Mehr als 20 Jahre IT im Krankenhäusern
- > 20 Jahre Datenschutz im Gesundheitswesen

Mitarbeit in wiss. Fachgesellschaften

- Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V. (GMDS)
- Gesellschaft für Datenschutz und Datensicherung e.V. (GDD)
- Gesellschaft für Informatik (GI)

Mitarbeit in Verbänden

- Berufsverband der Datenschutzbeauftragten Deutschlands e.V. (BvD)
- Bundesverband Gesundheits-IT e. V (bvitg)
- Fachverband Biomedizinische Technik e.V. (fbmt)
- HL7 Deutschland e.V.

Grundsätzlicher Hinweis

Virtuelle Seminare und Interaktion

Virtuelle Seminare stellen besondere Herausforderungen an die Interaktion miteinander.

Daher ein paar Worte vorab:

- Nach etwa der Hälfte der Zeit gibt es eine kurze Pause
- Einzelne Themenblöcke sind abgetrennt voneinander (Trennfolie mit Überschrift des folgenden Blockes)
- Bitte über Chat Verständnisfrage stellen
 - Nach jedem Block gibt es Zeit, **Verständnisfragen** zu dem gerade besprochenen Block zu stellen
- Zum Ende ist Zeit für grundsätzliche Fragen Diskussion eingeplant
- Aufgrund der hohen Anzahl Teilnehmer wird es absehbar nicht möglich sein, alle Fragen zu besprechen.
 - Bitte nutzen Sie auch die Mailadresse und kontaktieren Sie mich nach der Veranstaltung per E-Mail

Agenda

Was möchte ich vorstellen?

- Cloud:
Was ich darunter verstehe
- Cloud = Outsourcing: Die europäische Sicht
- Cloud und Verarbeitung im Ausland
 - Outsourcing von Sozialdaten: Vorgaben für Leistungsträger
 - Outsourcing und das Landesrecht für Krankenhäuser
 - § 203 StGB: Verbot der unbefugten Offenbarung
- Drittstaatentransfer
- Cloud: Sicherheit der Verarbeitung
- Dokumentationspflichten

Cloud:

Was ich darunter verstehe

Cloud Computing

Was ist das? Cloud Computing?

- Cloud Computing = „Form der Bereitstellung von
 - gemeinsam nutzbaren und
 - flexibel skalierbaren IT-Leistungen durch
 - nicht fest zugeordnete IT-Ressourcen
 - über Netze“
- Unterscheidung in
 - Private Cloud
 - Public Cloud
 - Hybrid Cloud (Gemeinsame Nutzung von Private und Public Cloud)

Cloud Computing

Ebenen des Cloud Computing

Angebot

Vertikale und horizontale
Anwendungen als Services
(SaaS)

Technische Frameworks
als Service
(PaaS)

IT-Basis Infrastruktur und
Hardware-Komponenten
als Service
(IaaS)

Software as a Service (SaaS)

Beispiele: Google Apps for Business,
Microsoft Online Services
(BPOS) und CRM Online,
Salesforce.com, WebEx, ...

Platform as a Service (PaaS)

Beispiele: Force.com, Google App
Engine, Microsoft Azure
Services (SQL Azure,
.NET Services)

Infrastructure as a Service (IaaS)

Beispiele: Amazon EC2, AppNexus,
HP Cloud Enabling
Computing, Microsoft
Windows Azure Platform,
Sun Cloud

Zielgruppe

- Business Analysts
- Fachabteilungen
- Wissensarbeiter
- Privatkunden

- Architekten und Entwickler
von Lösungen zur
Anwendungs- und
Geschäftsprozessintegration

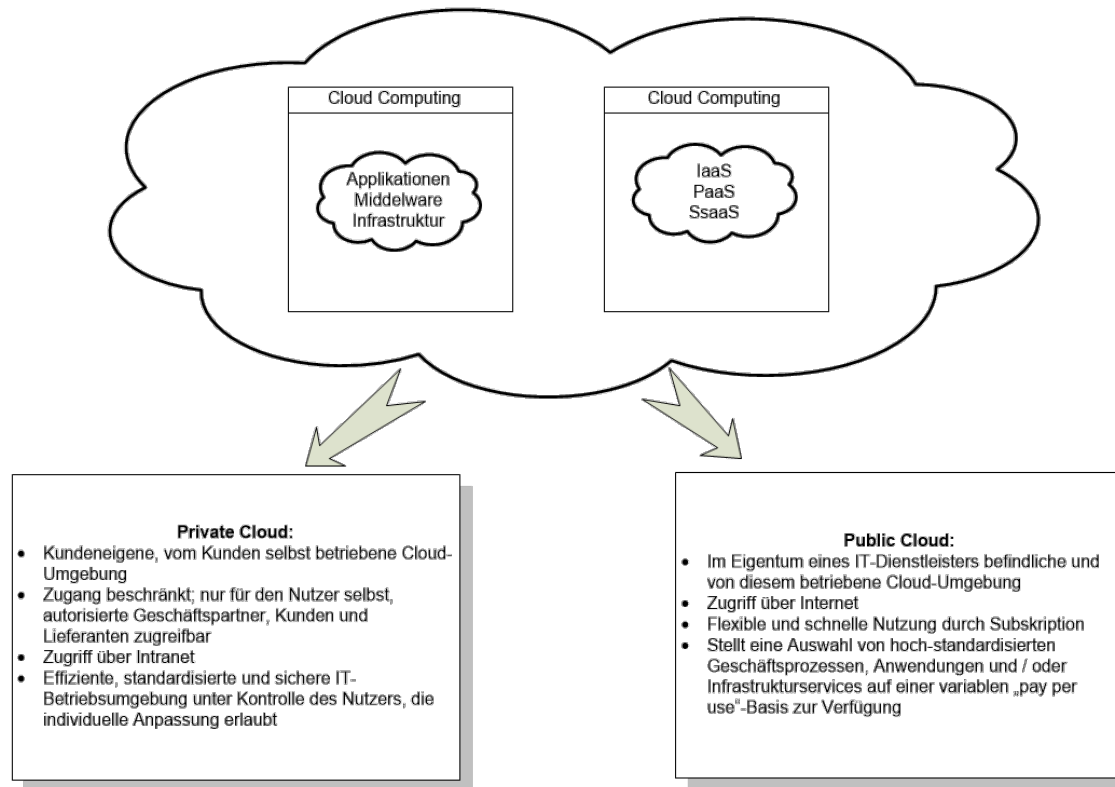
- IT-Betrieb / IT-Dienstleister,
- Cloud-Provider

Business

Informations- und
Telekommunikationstechnologie

Cloud Computing

Private Cloud vs. Public Cloud



Cloud Computing

Aus Sicht eines Datenschützers

- Private Cloud
 - In Eigenbetrieb in eigenen Räumlichkeiten: „Normale“ Verarbeitung
 - Mit Unterstützung durch Dienstleister:
„Normales“ Outsourcing = Verarbeitung im Auftrag
- Public Cloud/Hybrid-Cloud
 - Immer nur mit Dienstleister möglich:
„Normales“ Outsourcing = Verarbeitung im Auftrag
- Einzige Besonderheit bei Cloud:
 - Wo werden die Daten verarbeitet?

Cloud = Outsourcing: Die europäische Sicht

Zielrichtung der DS-GVO: Freier Verkehr personenbezogener Daten in der Union

KAPITEL I

Allgemeine Bestimmungen

Artikel 1

Gegenstand und Ziele

- (1) Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.
- (2) Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.
- (3) Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden.

Freier Verkehr der Daten wird nicht aus Datenschutzgründen eingeschränkt

- Art. 1 Abs. 3 DS-GVO:
 - „Der freie **Verkehr** personenbezogener **Daten in der Union** darf aus **Gründen des Schutzes natürlicher Personen bei der Verarbeitung** personenbezogener Daten **weder eingeschränkt noch verboten werden.**“
- Es ist dem nationalen Gesetzgeber nicht erlaubt, die Verarbeitung personenbezogener Daten *aus Datenschutzgründen* einzuschränken.
- Es ist dem nationalen Gesetzgeber jedoch erlaubt, dies aus anderen Gründen zu tun. Z.B.
 - Verarbeitung nur im Geltungsbereich des Grundgesetzes
 - Verarbeitung nur im Geltungsbereich des Strafgesetzbuches
 - Verarbeitung nur an Orten, die zur Sicherheit der Verarbeitung mindestens folgenden Anforderungen genügen: ...

Cloud und Verarbeitung im Ausland

Outsourcing von Sozialdaten: Vorgaben für Leistungsträger

Sozialdaten und Verarbeitung im Auftrag: Rechtliche Rahmenbedingungen

Vorab: Was sind Sozialdaten?

- § 67 Abs. 2 S. 1 SGB10:
„**Sozialdaten sind personenbezogene Daten** (Artikel 4 Nummer 1 der Verordnung (EU) 2016/679), die **von einer in § 35 des Ersten Buches genannten Stelle** im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch **verarbeitet werden.**“
- § 35 Abs. 1 SGB 1: benennt ausschließlich Leistungsträger sowie deren Verbände
- Sozialdaten fallen damit insbesondere bei (gesetzlichen) Krankenkassen an
- Leistungserbringer wie Krankenhäuser, Arztpraxen usw. verarbeiten i.d.R. keine Sozialdaten !

Sozialdaten und Verarbeitung im Auftrag: Rechtliche Rahmenbedingungen

§ 35 SGB 1: Das Sozialgeheimnis

- § 35 Abs. 6 SGB 1:
 - „Die **Absätze 1 bis 5 finden** neben den in Absatz 1 genannten Stellen auch **Anwendung auf** solche Verantwortliche oder deren **Auftragsverarbeiter**,
 - 1. die **Sozialdaten im Inland verarbeiten**, sofern die Verarbeitung nicht im Rahmen einer Niederlassung in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erfolgt, oder
 - 2. die **Sozialdaten im Rahmen der Tätigkeiten einer inländischen Niederlassung** verarbeiten.“
- Vorgaben aus § 35 Abs. 1 bis 5 SGB 1 gelten auch für Auftragsverarbeiter
- In § 35 Abs. 1 SGB 1 genannten **Leistungsträger dürfen Auftragsverarbeiter nur beauftragen, wenn die Vorgaben** der Sozialgesetzbücher von diesen Auftragsverarbeitern auch **eingehalten werden (können)**

Sozialdaten und Verarbeitung im Auftrag: Rechtliche Rahmenbedingungen

§ 35 SGB 1: Das Sozialgeheimnis

- § 35 Abs. 2 SGB 1:
 - Verarbeitung von Sozialdaten ist in den Sozialgesetzbüchern abschließend geregelt (abgesehen von Geltung der DS-GVO)
 - Andere Regelungen **insbesondere Regelungen bzgl. Herausgabe von Sozialdaten an behördliche Stellen**, die nicht in einem Sozialgesetzbücher und insbesondere in §§ 67dff SGB 10 geregelt sind, **dürfen nicht beachtet und befolgt werden**

Sozialdaten und Verarbeitung im Auftrag: Rechtliche Rahmenbedingungen

§ 35 SGB 1: Das Sozialgeheimnis

- § 35 Abs. 3 SGB 1:
„Soweit eine **Übermittlung von Sozialdaten nicht zulässig ist, besteht keine Auskunftspflicht, keine Zeugnispflicht und keine Pflicht zur Vorlegung oder Auslieferung von** Schriftstücken, nicht automatisierten Dateisystemen und automatisiert verarbeiteten **Sozialdaten.**“
- Regelungen von § 35 Abs. 2, 3 SGB 1
 - Gelten für deutsche Behörden
 - **Gelten** insbesondere natürlich **auch für normative/gesetzliche Regelungen im Ausland**, denen ggf. ein Auftragsverarbeiter unterliegt
- **Unterliegt ein Auftragsverarbeiter ausländischem Recht**, welches den Auftragsverarbeiter zwingt, **entgegen geltendem deutschen Recht Sozialdaten an ausländische Behörden zu übermitteln**, so erscheint eine rechtskonforme **Beauftragung kaum möglich**

Sozialdaten und Verarbeitung im Auftrag: Rechtliche Rahmenbedingungen

§ 35 SGB 1: Das Sozialgeheimnis

- § 35 Abs. 2a SGB 1:
„Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.“
- **Auftragsverarbeiter bzw. dessen Beschäftigte**, die Sozialdaten im Auftrag verarbeiten (könnten), **müssen auf die Einhaltung des Sozialgeheimnisses verpflichtet werden**
 - Auf entsprechende vertragliche Regelung achten!
 - Dabei auch an Vorgabe aus § 35 Abs. 1 SGB 1 denken:
„Die Beschäftigten haben auch nach Beendigung ihrer Tätigkeit bei den genannten Stellen das Sozialgeheimnis zu wahren.“

Sozialdaten und Verarbeitung im Auftrag: Rechtliche Rahmenbedingungen

§ 35 SGB 1: Das Sozialgeheimnis

- § 35 Abs. 4 SGB 1:
„**Betriebs- und Geschäftsgeheimnisse stehen Sozialdaten gleich.**“
- § 67 Abs. 2 S. 2 SGB 10
„**Betriebs- und Geschäftsgeheimnisse** sind **alle betriebs- oder geschäftsbezogenen Daten**, auch von juristischen Personen, die Geheimnischarakter haben.“
 - Also z.B. Beschäftigungsverhältnisse oder Vertragsgestaltungen
- **Regelungen zum Schutz von Sozialdaten gelten 1:1 auch für Betriebs- und Geschäftsgeheimnisse der beauftragenden Leistungsträger**
- Dies betrifft natürlich auch das Outsourcing und damit insbesondere auch die Nutzung einer Cloud

Sozialdaten und Verarbeitung im Auftrag: Rechtliche Rahmenbedingungen

§ 80 SGB 10: Verarbeitung von Sozialdaten im Auftrag

– § 80 Abs. 1 SGB 10:

Die Erteilung eines Auftrags i.S.d. Art. 28 DS-GVO ist nur zulässig, wenn der Verantwortliche seiner Rechts- oder Fachaufsichtsbehörde **rechtzeitig vor der Auftragserteilung**

1. den **Auftragsverarbeiter**, die bei diesem vorhandenen **technischen und organisatorischen Maßnahmen und ergänzenden Weisungen**,
2. die **Art der Daten**, die im Auftrag verarbeitet werden sollen, und den **Kreis der betroffenen Personen**,
3. die **Aufgabe**, zu deren Erfüllung die Verarbeitung der Daten im Auftrag erfolgen soll, sowie
4. den **Abschluss von etwaigen Unterauftragsverhältnissen schriftlich oder elektronisch anzeigt**.

– Auftragsverarbeitung ist für Leistungsträger anzeigepflichtig!

Sozialdaten und Verarbeitung im Auftrag: Rechtliche Rahmenbedingungen

§ 80 SGB 10: Verarbeitung von Sozialdaten im Auftrag

- § 80 Abs. 1 SGB 10 = Rahmenbedingung für Unterauftragsverhältnisse
- Allgemeine Zustimmung zu Unterauftragsverarbeiter ist Leistungserträgen regelhaft nicht möglich
- Leistungsträger müssen Unterauftragsverarbeiter vor Vertragsabschluss bzw. vor Änderung von Unterauftragsverhältnissen melden!
- (Potentielle) Auftragsverarbeiter von Sozialdaten sollten sich daher Prozesse überlegen, wie sie ihren Auftragsgebern (z.B. Krankenkassen) die Einhaltung dieser Pflicht ermöglichen

Cave:

- Es müssen die (Unter-)Auftragsverarbeiter benannt werden, die mit der Verarbeitung der Sozialdaten tatsächlich einbezogen werden
- **Verweis auf allgemeine Listen im Internet reichen nicht zur Erfüllung der gesetzlichen Pflicht**

Sozialdaten und Verarbeitung im Auftrag: Rechtliche Rahmenbedingungen

§ 80 SGB 10: Verarbeitung von Sozialdaten im Auftrag

- § 80 Abs. 2 SGB 10:
„Der Auftrag zur Verarbeitung von Sozialdaten darf nur erteilt werden, wenn die Verarbeitung im Inland, in einem anderen Mitgliedstaat der Europäischen Union, in einem diesem nach § 35 Abs. 7 SGB 1 gleichgestellten Staat, oder, sofern ein Angemessenheitsbeschluss gemäß Art. 45 DS-GVO vorliegt, in einem Drittstaat oder in einer internationalen Organisation erfolgt.“
- § 35 Abs. 7 SGB 1: Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum und die Schweiz

Sozialdaten und Verarbeitung im Auftrag: Rechtliche Rahmenbedingungen

§ 80 SGB 10: Verarbeitung von Sozialdaten im Auftrag

- § 80 Abs. 2 SGB 10: **Beschränkung der Verarbeitung von Sozialdaten im Ausland**
- Auslandsverarbeitung also ausschließlich, wenn die **Verarbeitung ausschließlich in**
 - **EU**
 - Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum (**EWR**)
 - **Schweiz**
 - **Drittstaat mit Angemessenheitsbeschluss der EU Kommission***

Zur Zeit sind dies

- Andorra, Argentinien, Kanada (kommerzielle Organisationen), Färöer-Inseln, Guernsey, Israel, Isle of Man, Japan, Jersey, Neuseeland, Republik Korea, Schweiz, Vereinigtes Königreich im Rahmen der GDPR und der LED sowie Uruguay

erfolgt.

* Europäische Kommission: Adequacy decisions, online unter

https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_de?msclkid=d9dca4c2cf6411ecb9273a996a1bc628

Sozialdaten und Verarbeitung im Auftrag: Rechtliche Rahmenbedingungen

§ 80 SGB 10: Verarbeitung von Sozialdaten im Auftrag

– § 80 Abs. 3 SGB 10:

„Die **Erteilung eines Auftrags** zur Verarbeitung von Sozialdaten durch nicht-öffentliche Stellen ist **nur zulässig, wenn**

1. beim Verantwortlichen sonst **Störungen im Betriebsablauf auftreten können** oder
2. die **übertragenen Arbeiten** beim Auftragsverarbeiter **erheblich kostengünstiger** besorgt werden können.

Dies gilt nicht, wenn Dienstleister in der Informationstechnik, deren absolute Mehrheit der Anteile oder deren absolute Mehrheit der Stimmen dem Bund oder den Ländern zusteht, mit vorheriger Genehmigung der obersten Dienstbehörde des Verantwortlichen beauftragt werden.“

Sozialdaten und Verarbeitung im Auftrag: Rechtliche Rahmenbedingungen

§ 80 SGB 10: Verarbeitung von Sozialdaten im Auftrag

§ 80 Abs. 3 SGB 10: Leistungsträger muss Verarbeitung im Auftrag rechtfertigen

– Schutzzweck Norm = weitgehenden Reduzierung der Fälle von Datenverarbeitung durch andere Stellen als öffentliche Stellen

– Daher eng auszulegen*

a) Störungen im Betriebsablauf

- Welche Störungen können ohne Auftragsverarbeitungen auftreten, die mit Outsourcing aus welchen Gründen vermieden werden können?
- Wie wirken sich diese Störungen im Betriebsablauf aus?
- Störungen im Betriebsablauf:*
 - Abwicklung der Leistungen zu Lasten des Leistungsempfängers werden ohne Auftragsverarbeitung verzögert

* So z.B. Herbst § 80 Rn. 58, 59. In: Kasseler Kommentar Sozialversicherungsrecht, Werkstand: 117. EL Dezember 2021

Sozialdaten und Verarbeitung im Auftrag: Rechtliche Rahmenbedingungen

§ 80 SGB 10: Verarbeitung von Sozialdaten im Auftrag

§ 80 Abs. 3 SGB 10: Leistungsträger muss Verarbeitung im Auftrag rechtfertigen

b) **Erheblich** kostengünstiger

- Es reicht nicht, dass Aufträge vom Dienstleister kostengünstiger erledigt werden
- Es muss erheblich kostengünstiger erfolgen
- „Erheblich“ gesetzlich nicht definiert, daher Einzelfallprüfung
- Vergleichsberechnung hinsichtlich der zu erwartenden Kosten erforderlich
- Bei Beurteilung zu beachten*
 - Gesetzeszweck beachten = weitgehenden Begrenzung der Datenverarbeitung durch nicht-öffentliche Stellen
 - Schutzbedarf von Sozialdaten sehr hoch
 - Es muss sich eine **Ersparnis** ergeben, die bei **objektiver Betrachtung** die **eigene Datenverarbeitung** schlichtweg **unwirtschaftlich und unverhältnismäßig erscheinen lässt**

* So z.B. Herbst § 80 Rn. 60. In: Kasseler Kommentar Sozialversicherungsrecht, Werkstand: 117. EL Dezember 2021

Sozialdaten und Verarbeitung im Auftrag: Rechtliche Rahmenbedingungen

§ 80 SGB 10: Verarbeitung von Sozialdaten im Auftrag

- § 80 Abs. 3 SGB 10: Leistungsträger muss Verarbeitung im Auftrag rechtfertigen
- Zu beachten:
 - § 80 Abs. 5 SGB 10 schränkt § 80 Abs. 3 SGB 10 ein:
„**Absatz 3 gilt nicht** bei Verträgen über die **Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen** durch andere Stellen im Auftrag, bei denen ein Zugriff auf Sozialdaten nicht ausgeschlossen werden kann.“
 - Aber Vorgabe von § 80 Abs. 5 S. 2 SGB 10 beachten:
„**Die Verträge sind** bei zu erwartenden oder bereits eingetretenen Störungen im Betriebsablauf **unverzüglich der Rechts- oder Fachaufsichtsbehörde mitzuteilen.**“

Sozialdaten und Verarbeitung im Auftrag: Rechtliche Rahmenbedingungen

§ 80 SGB 10: Verarbeitung von Sozialdaten im Auftrag

- § 80 Abs. 4 S. 2 SGB 10
 - „Ist der **Auftragsverarbeiter** eine nicht-öffentliche Stelle, **unterliegt** dieser der Aufsicht **der gemäß § 40 des Bundesdatenschutzgesetzes zuständigen Behörde.**“
- Auftragsverarbeiter unterliegt grundsätzlich der deutschen Datenschutzaufsicht, anderslautende vertragliche Gestaltungen sind nichtig
- Auftragsverarbeiter = nicht-öffentliche Stelle
 - Die nach Landesrecht zuständige Aufsichtsbehörde ist zuständig für die Überwachung der Einhaltung der sozialrechtlichen Datenschutzbestimmungen beim Auftragsverarbeiter
 - Für den Leistungsträger i.d.R. Bundesdatenschutzbeauftragte(r)
 - Nach § 40 Abs. 2 BDSG werden ggf. beide Aufsichtsbehörden gemeinsam zuständig sein und Fälle gemeinsam bearbeiten

Sozialdaten und Verarbeitung im Auftrag: Rechtliche Rahmenbedingungen

Ergänzende Hinweise: Auswirkungen des Schrems II Urteils

Auslandsverarbeitung und EuGH Urt. v. 16.07.2020, Az. C-311/18* („Schrems II)

- Rn. 87: Die etwaige Verarbeitung der betreffenden Daten durch ein Drittland für Zwecke der öffentlichen Sicherheit, der Landesverteidigung und der Sicherheit des Staates stellt die Anwendbarkeit der DSGVO auf die fragliche Übermittlung nicht in Frage.
- Rn. 92: Schutzniveau der DS-GVO muss bei Übermittlung gewährleistet werden
- Rn. 105: Erforderliche Garantien bei Drittstaatenverarbeitung müssen „erforderlichen geeigneten Garantien, durchsetzbaren Rechte und wirksamen Rechtsbehelfe gewährleisten“ beinhalten.
- Rn. 105: Bei der Zusammenhang mit einer solchen (möglichen) Übermittlung vorzunehmenden Beurteilung sind insbesondere die vertraglichen Regelungen zu berücksichtigen
- Rn. 105: Prüfung vertraglicher Regelungen muss insbesondere einen etwaigen Zugriff der Behörden dieses Drittlands auf die übermittelten personenbezogenen Daten beinhalten

* EuGH Urt. v. 16.07.2020, Az. C-311/18, Online unter <https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1>

Sozialdaten und Verarbeitung im Auftrag: Rechtliche Rahmenbedingungen

Ergänzende Hinweise: Auswirkungen des Schrems II Urteils

- Bei Prüfung von Verträgen zur Verarbeitung von Sozialdaten im Auftrag sind selbstverständlich auch die Vorgaben des Schrems II Urteils zu beachten
- Insbesondere zu prüfen:
 - Unterliegt der Auftragsverarbeiter rechtlichen Bestimmungen in einem Drittland, welches eine nach deutschem (Sozial)Recht rechtswidrige Offenbarung von Sozialdaten ermöglichen könnte?

Sozialdaten und Verarbeitung im Auftrag: Rechtliche Rahmenbedingungen

Ergänzende Hinweise: Rechtswahl

- § 35 Abs. 2 SGB 1:
Verarbeitung von Sozialdaten ist in den Sozialgesetzbüchern abschließend geregelt
- Fremdes Recht grundsätzlich nicht anwendbar
- Fazit:
 1. Deutsches Recht ist bei der Vertragsgestaltung insbesondere für Leistungsträger zwingend erforderlich
 2. Verträge zur Verarbeitung von Sozialdaten im Auftrag müssen zwingend deutsches Recht vorsehen*

* Hinweis: Im reinen B2B-Kontext ist sehr umstritten, ob eine Rechtswahl zwingende deutsche Rechtsvorschriften nach Art. 3 Abs. 3 Rom I-VO überhaupt außer Kraft setzen kann. Auch außerhalb der Verarbeitung von Sozialdaten sollte man dies daher beachten. Diskussion zum Thema z.B. Ehlen/Blum, CR 2022, 10-15

Sozialdaten und Verarbeitung im Auftrag: Rechtliche Rahmenbedingungen

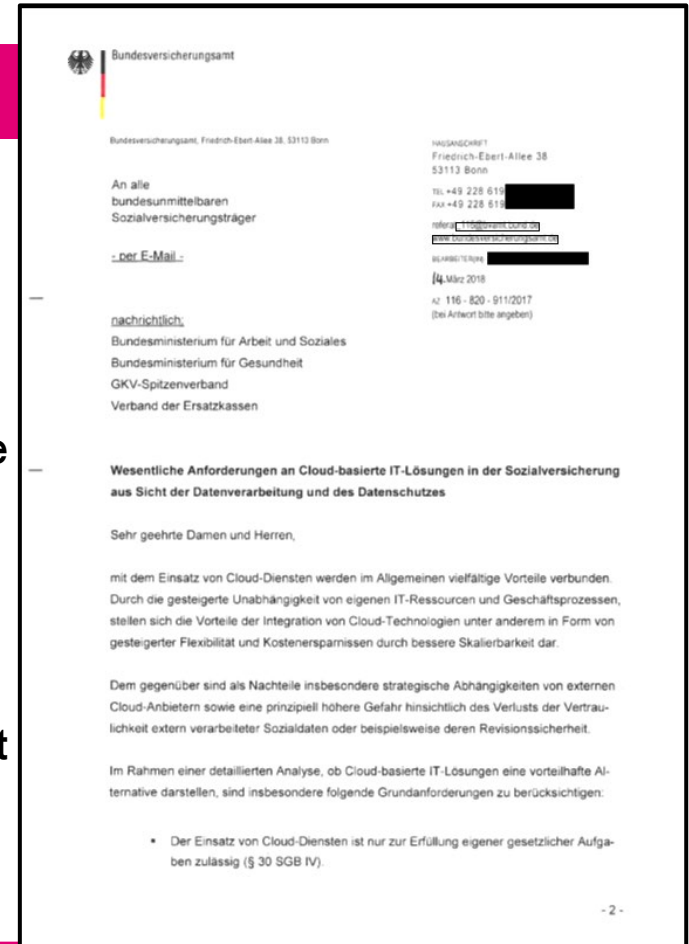
Ergänzende Hinweise: Gerichtsstand

- § 51 Abs. 1 Sozialgerichtsgesetz:
Gerichte der Sozialgerichtsbarkeit entscheiden über öffentlich-rechtliche Streitigkeiten
- § 51 Abs. 2 Sozialgerichtsgesetz:
Gerichte der Sozialgerichtsbarkeit entscheiden auch über privatrechtliche Streitigkeiten in Angelegenheiten der Zulassung von Trägern und Maßnahmen durch fachkundige Stellen
- Fazit:
 1. Deutscher Gerichtsstand ist bei der Vertragsgestaltung insbesondere für Leistungsträger zwingend erforderlich
 2. Verträge zur Verarbeitung von Sozialdaten im Auftrag müssen zwingend als Gerichtsstand deutsche Gerichte vorsehen

Cloud also grundsätzlich erlaubt, aber Besonderheiten sind zu beachten ...

Bundesversicherungsamt: Vorgaben beachten

- Bundesversicherungsamt, Rundschreiben vom 14. März 2018
- Mit Einsatz von Cloud-Diensten werden im Allgemeinen vielfältige Vorteile verbunden
 - U.a.: **gesteigerte Flexibilität** und **Kostensparnisse** durch bessere Skalierbarkeit
- Aber auch diverse Nachteile
 - U.a. **strategische Abhängigkeiten** von externen Cloud-Anbietern sowie eine prinzipiell höhere **Gefahr hinsichtlich des Verlusts der Vertraulichkeit** extern verarbeiteter Sozialdaten oder beispielsweise **deren Revisionsicherheit**



Cloud also grundsätzlich erlaubt, aber Besonderheiten sind zu beachten ...

Bundesversicherungsamt: Vorgaben beachten

Fazit: Ja, aber

- Der Einsatz von Cloud-Diensten ist nur zur **Erfüllung eigener gesetzlicher Aufgaben** zulässig (§ 30 SGB IV).
- Sofern Sozialdaten in externen Cloud-Lösungen verarbeitet werden sollen, kann dies nur auf **Grundlage einer Auftragsdatenverarbeitung** erfolgen (§ 80 SGB 10 i. V. m. Artikel 28 DSGVO)
- Je nach Gestaltung der Vereinbarung **müssen** dabei auch **vertraglich in Bezug genommene Unterlagen (z. B. Service-Bedingungen)** vor dem **Hintergrund der Anforderungen bewertet werden**
- Für eine **Verarbeitung besonderer Arten personenbezogener Daten** sind besondere **Schutzmaßnahmen auf Grundlage einer eigenen Risikoanalyse** zu treffen
- Soweit eine Nutzung externer Cloud-Dienste zulässig ist, **muss** insbesondere vor dem Hintergrund der eingangs erwähnten strategischen Abhängigkeit eine **Wirtschaftlichkeitsanalyse erfolgen**

Outsourcing und das Landesrecht für Krankenhäuser

Deutschland: Gelebter Föderalismus

Krankenhäuser und Landesregelungen: Anwendungsbereich beachten

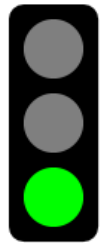
- Anwendungsbereich der Landesregelungen in der Regel auf Krankenhäuser beschränkt, welche dem Krankenhausfinanzierungsgesetz unterliegen
 - Aber Ausnahmen: § 2 LKG Berlin legt den Anwendungsbereich auf alle Krankenhäuser Berlins fest
- Einige Landesgesetze gelten nicht für Kirchen und Religionsgemeinschaften, wenn diese eigene Regelungen für Krankenhäuser erlassen haben
 - Kirchen erließen i.d.R. keine bereichsspezifischen Regelungen für Krankenhäuser, so dass die Landeskrankenhausgesetze angewendet werden
- Weiterhin werden mitunter Krankenhäuser des Bundes von den Landesregelungen ausgenommen
 - Bundeswehrkrankenhäuser unterliegen i.d.R. eigenen Rahmenbedingungen wie z.B. Soldatengesetz

Deutschland: Gelebter Föderalismus

Für Krankenhäuser in der Regel Landesgesetzgeber zuständig

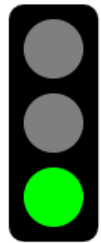
- Legaldefinition Krankenhäuser § 107 Abs. 1 SGB V
 - „Krankenhäuser im Sinne dieses Gesetzbuchs sind Einrichtungen, die
 1. der Krankenhausbehandlung oder Geburtshilfe dienen,
 2. fachlich-medizinisch unter ständiger ärztlicher Leitung stehen, über ausreichende, ihrem Versorgungsauftrag entsprechende diagnostische und therapeutische Möglichkeiten verfügen und nach wissenschaftlich anerkannten Methoden arbeiten,
 3. mit Hilfe von jederzeit verfügbarem ärztlichem, Pflege-, Funktions- und medizinisch-technischem Personal darauf eingerichtet sind, vorwiegend durch ärztliche und pflegerische Hilfeleistung Krankheiten der Patienten zu erkennen, zu heilen, ihre Verschlimmerung zu verhüten, Krankheitsbeschwerden zu lindern oder Geburtshilfe zu leisten,und in denen
 4. die Patienten untergebracht und gepflegt werden können.“

Landesrecht und Outsourcing: Länder, bei denen med. Daten im Auftrag verarbeitet werden dürfen



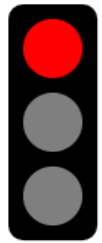
	Bremen	BaWü	Brandenburg	Hamburg
Gesetzliche Regelung	Bremisches Krankenhausdatenschutzgesetz	Landeskrankenhausgesetz Baden-Württemberg	Gesetz zur Entwicklung der Krankenhäuser im Land Brandenburg	Hamburgisches Krankenhausgesetz
Auftragsverarbeitung	<p>§ 10 AV erlaubt, wenn</p> <ul style="list-style-type: none"> • Wahrung Vorgaben BremKHDSG bei An-gewährleistet • AN unterwirft sich Kontrolle Landesbeauftragter DS • TOM berücksichtigen Vorgaben nach § 7 Abs. 4 BremDSG 	<p>AV unter bestimmten Voraussetzungen erlaubt, § 48:</p> <ul style="list-style-type: none"> • Benachrichtigung Daten-schutzaufsichtsbehörde • Schweigepflicht, § 203 StGB • TOM schriftlich vereinbart • Daten müssen Gewahrsam Krkh bleiben 	Keine spezifische Regelung, DS-GVO gilt	Keine spezifische Regelung, DS-GVO gilt
Besonderheiten	Bei Prüfung/Wartung von DV-Anlagen muss Krankenhaus Patientendaten im Einzelfall freigeben, genereller Zugriff nicht statthaft	<ul style="list-style-type: none"> • TOM müssen § 3 LDSG oder § 22 Abs. 2 BDSG entsprechen • §43: Für KH des Bundes und der Kirchen gelten deren Datenschutz Vorschriften 	TOM müssen § 24 LDSG sowie § 22 Abs. 2 BDSG abdecken	§ 11 Abs. 2: Verfahren der Übermittlung ist aufzuzeichnen

Landesrecht und Outsourcing: Länder, bei denen med. Daten im Auftrag verarbeitet werden dürfen



	Hessen	Niedersachsen	Rheinland-Pfalz	Sachsen
Gesetzliche Regelung	Hessisches Krankenhausgesetz 2011	Niedersächsisches Datenschutzgesetz	Landeskrankenhaus-gesetz	Sächsisches Krankenhausgesetz
Auftragsverarbeitung	Keine spezifische Regelung, DS-GVO gilt	AV unter Voraussetzungen § 17 erlaubt:: <ul style="list-style-type: none"> • Sicherstellung Feststellbarkeit, ob und von wem Daten verarbeitet wurden • Beschränkung Befugnisse auf erforderliche Maß • Sensibilisierung der Personen 	§ 36 Abs. 9, DS-GVO gilt	<ul style="list-style-type: none"> • AV bedarf der Zustimmung der zuständigen Behörde • Verarbeiter muss Schweigepflicht (§ 203 StGB) einhalten • Verarbeiter muss DSB benennen
Besonderheiten		In § 17 Abs. 3 genannte Maßnahmen sind zu beachten		Beauftragung eines Auftragnehmers, der seinen Sitz außerhalb der Europäischen Union hat, i.d.R. nicht möglich

Landesrecht und Outsourcing: Länder, bei denen med. Daten faktisch nicht verarbeitet werden dürfen



	Bayern*	Berlin
Gesetzliche Regelung	Bayerisches Krankenhausgesetz	Landeskrankenhausgesetz
Auftragsverarbeitung	AV außerhalb Krkh. nur zur verwaltungsmäßigen Abwicklung der Behandlung der Patienten erforderliche Daten, keine med. Daten.	<ul style="list-style-type: none"> • § 24(6) n.F. Wartung-/ Administrationstätigkeiten erlaubt • Sonstige AV nach § 24(7) LKG** <ul style="list-style-type: none"> a) Nur durch Krkh. b) Nur durch gleiche Unternehmensgruppe c) Andere Stellen AV nur, wenn kein Datenzugriff
Besonderheiten	TOM müssen gewährleisten, dass Patientendaten nicht unberechtigt verwendet oder übermittelt werden können.	<ul style="list-style-type: none"> • AV-Vertrag zur Wartung/ Admin-Tätigkeit nach Wortlaut LKG n.F. nicht erlaubt • Auftragsverarbeiter haftet gegenüber AG für Pflichtverletzungen der Unterauftragnehmer

* Änderung bay. Landeskrankenhausgesetz am 26.4.2022 beschlossen, Änderung tritt 1. Juni 2022 in Wirkung: Protokoll der Landtagssitzung <https://www.bayern.landtag.de/webangebot2/webangebot/protokolle;execution=e1s1>,

Gesetzesvorschlag und Änderungsanträge <https://www.bayern.landtag.de/webangebot2/webangebot/vorgangsanzeige?wp=18&drsnr=19685>

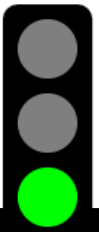
** § 24 Abs. 7 LKG Berlin tritt mit Wirkung vom 25.10.2022 in Wirkung

Landesrecht und Outsourcing: Ja, aber...



	Mecklenburg-Vorpommern	NRW	Saarland	Sachsen-Anhalt	Schleswig-Holstein	Thüringen
Gesetzliche Regelung	Landeskrankenhausgesetz	Gesundheitsdatenschutzgesetz	Saarländisches Krankenhausgesetz	Krankenhausgesetz Sachsen-Anhalt	Landeskrankenhausgesetz (Entwurf)	Thüringer Krankenhausgesetz
Auftragsverarbeitung	<p>§ 38 LKHG M-V, Voraussetzung</p> <ul style="list-style-type: none"> Vermeidung der Störung im Betrieb erhebliche Kostenersparnis Einhaltung § 203 StGB Verarbeitung außerhalb Geltungsbereich GG = Einwilligung des Patienten 	<p>AV unter bestimmten Voraussetzungen erlaubt:</p> <ul style="list-style-type: none"> Vermeidung der Störung im Betrieb erhebliche Kostenersparnis 	<p>§ 13a, erlaubt wenn</p> <ul style="list-style-type: none"> Vermeidung der Störung im Betrieb erhebliche Kostenersparnis Vorherige Prüfpflicht, ob verschlüsselte/pseudonymisierte Daten genutzt werden können AN unterwirft sich Kontrolle Landesbeauftragter DS 	<p>§ 16 Abs. 4</p> <ul style="list-style-type: none"> Wahrung Schweigepflicht Schutzwürdige Belange des Patienten oder des Betroffenen werden nicht beeinträchtigt Der Patient ist vorab über die AV zu informieren und hat Widerspruchsrecht 	<p>§ 37 LKHG-E, Voraussetzung</p> <ul style="list-style-type: none"> Vermeidung der Störung im Betrieb erhebliche Kostenersparnis Auftragsverarbeitung mit anonymen Daten, wenn nicht möglich, dann mit pseudonymen Daten Verarbeitung nur EU 	<p>§ 27b AV erlaubt wenn</p> <ul style="list-style-type: none"> Ohne AV Störungen im Betriebsablauf nicht vermieden werden können erhebliche Kostenersparnis Verarbeiter muss ThürKHG und Schweigepflicht § 203 StGB einhalten AV vor Auftragserteilung unter Vorlage TOM bei der Behörde schriftlich anzeigen
Besonderheiten	<p>Eine über 3 Monate hinausgehende Speicherung von Patientendaten durch einen Auftragnehmer außerhalb des Krankenhauses ist nur zulässig, wenn die Patientendaten auf getrennten Datenträgern gespeichert sind, die der Auftragnehmer für den Krankenhausträger verwahrt</p>	<ul style="list-style-type: none"> Patientendaten (klinisch) sind vom AN auf physisch getrennten Dateien zu verarbeiten. AN muss sich der Kontrolle durch den Landesbeauftragten für den Datenschutz unterwerfen 	<p>Eine über 3 Monate hinausgehende Speicherung von Patientendaten durch einen Auftragnehmer außerhalb des Krankenhauses ist nur zulässig, wenn die Patientendaten auf getrennten Datenträgern gespeichert sind, die der Auftragnehmer für den Krankenhausträger verwahrt</p>	<ul style="list-style-type: none"> Wie wird Patient vor AV informiert? Wie wird mit dem Widerspruch eines Patienten umgegangen? 	<p>AV nur mit anonymen oder pseudonymen Daten</p>	<ul style="list-style-type: none"> § 27b gilt auch für Fernwartung Kontrollen durch AG oder Datenschutzaufsicht sind jederzeit zu ermöglichen

Der Vollständigkeit halber: Bund und Kirche



	Bundeswehrkrankenhäuser, Patientendaten Nicht-Soldaten	Ev. Kirche	Kath. Kirche
Gesetzliche Regelung	BDSG und Landesrecht für Krankenhäuser	DSG-EKD	Grundsätzlich kann jedes Bistum eigenes Recht erlassen, daher KDG in jedem Bistum veröffentlicht Gesetz über den Kirchlichen Datenschutz (KDG); entspricht weitestgehend DS-GVO Durchführungsverordnung zum KDG (KDG-DVO)
Auftragsverarbeitung	Art. 28 DS-GVO bzw. je nach Landesrecht entsprechende Vorschrift	§ 30 DSG-EKD; Anforderung weitestgehend Art. 28 DS-GVO	<ul style="list-style-type: none"> • § 29 KDG • § 21 KDG-DVO
Besonderheiten	<ul style="list-style-type: none"> • Die meisten Bundeswehrkrankenhäuser behandeln auch Nicht-Soldaten, einige haben Kooperationsverträge mit Krankenhäuser und Praxen • Teilnahme an der stationären/teilstationären Versorgung eröffnet je nach Landesrecht den Anwendungsbereich für das jeweilige Landesrecht für Krankenhäuser 	<ul style="list-style-type: none"> • Keine speziellen bundesweiten Regelungen für Krankenhäuser, aber einige Kirchen erließen ergänzende Regelungen; i.d.R. Landeskrankenhausgesetze zu beachten • § 26 DSG-EKD Regelung Datengeheimnis inkl. Verpflichtungsvorschrift • Zwingend bei nichtkirchlichen Auftragnehmern: Unterzeichnung „Unterwerfungserklärung“ (kirchl. Datenschutzaufsicht wird von Auftragnehmer anerkannt) • Kirche hat Muster-AV-Vertrag bereitgestellt, aber keine Pflicht, diesen zu verwenden • Ev. Kirche hat eigene IT-Sicherheitsverordnung, bei Abbildung TOM beachten 	<ul style="list-style-type: none"> • Keine speziellen bundesweiten Regelungen für Krankenhäuser, aber einige Kirchen erließen ergänzende Regelungen; i.d.R. Landeskrankenhausgesetze zu beachten • Fernwartung von IT-Systemen darf nur erfolgen, wenn der Beginn aktiv seitens des Auftraggebers eingeleitet wurde und die Fernwartung systemseitig protokolliert wird • § 5 KDG Regelung Datengeheimnis inkl. Verpflichtungsvorschrift • Beschluss der Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschland bzgl. AN, die nicht der Kirche angehören: <ul style="list-style-type: none"> – KDG muss in AV-Vertrag aufgenommen werden – § 31 KDG muss erfüllt werden

Landesrecht und Outsourcing: die europäische Sicht

Für Krankenhäuser in der Regel Landesgesetzgeber zuständig

- Einschränkende Regelungen in MV, NRW, Saarland, Sachsen-Anhalt, Schleswig-Holstein und Thüringen wohl europarechtskonform
 - Entweder als konkretisierende bzw. ergänzende Maßnahme zu Art. 32 DS-GVO
 - oder als Beschränkung i.S.v. Art. 9 Abs. 4 DS-GVO anzusehen
- Ortsbeschränkungen in Berlin und (Bayern) wohl europarechtswidrig
- Aber rechtliche Vorgaben sind vom Rechtsanwender zu befolgen, bis
 - a) der Gesetzgeber die Regelungen ändert oder
 - b) ein Gericht die Regelungen für unvereinbar mit deutschem Recht beurteilt und die Regelungen für ungültig erklärt

Cloud: Ein paar Hinweise

Verschiedene Aspekte zu betrachten, z.B.

- Vertragsrechtliche Fragen klären, z.B.
 - Darf ich Outsourcing betreiben?
Existieren bspw. widersprechende landeskrankenhausspezifische Regelungen?
 - Ausweitung Behandlungsvertrag, wenn Cloud außerhalb Deutschlands betrieben wird?
 - Stichwort: Muss der Patient damit rechnen, dass die Patientendaten ggf. in einem Land verarbeitet werden, wo das deutsche Recht nicht gilt?
(Unabhängig von der Frage, ob entsprechende Vereinbarungen im Behandlungsvertrag dem AGB-Recht entsprechen würden)
- Einhaltung Vorgaben Strafrecht wie beispielsweise
 - Wie wird eine nach § 203 StGB erfolgte unbefugte Offenbarung im Ausland verfolgt? (kommt gleich)

Cloud: Ein paar Hinweise

Fragen aus dem Datenschutzrecht, wie beispielsweise

- Regelhaft wird es sich um Verarbeitung im Auftrag handeln, in Einzelfällen (z.B. Forschung) ggf. auch um Gemeinsam Verantwortliche nach Art. 26 DS-GVO
 - Zu prüfen: Können die eigenen Pflichten, die bei der Verarbeitung ggf. der Cloud-Anbieter erfüllen muss, überhaupt vertraglich weitergegeben werden?
 - Kann das Risiko für betroffene Personen ausreichend genau dargestellt werden, um den Informationspflichten nach Artt. 13, 14 DS-GVO zu genügen?
Wie geht man bzgl. Informationspflichten mit früheren Patienten um?
- Cloud-Anbieter außerhalb Europas
 - Wie wird nach dem EuGH Schrems II Urteil ein dem EU Recht entsprechendes Datenschutzniveau gewährleistet?

§ 203 StGB: Verbot der unbefugten Offenbarung

§ 203 StGB: Verarbeitung im Ausland

Schutzzweck des § 203 StGB?

- Vordergrund § 203 StGB:
 - Individualinteresse an der Geheimhaltung bestimmter Tatsachen
 - Der Geheimnisträger kann über das Geheimnis disponieren
- Aber auch:
 - Allgemeininteresse an der Verschwiegenheit von Amtsträgern
 - Vertrauen der Bevölkerung stärken, dass Personen, welche in die Privatsphäre eindringen, diese Geheimnisse wahren
- Reichweite
 - Geschützt sind **fremde Geheimnisse, auch „Bagatellinformationen“ oder illegale Geheimnisse**
 - Offenkundige Tatsachen fallen nicht unter den Schutz

§ 203 StGB: Verarbeitung im Ausland

Adressaten des § 203 StGB im Gesundheitswesen

- Angehörigen eines Unternehmens der privaten Kranken-, Unfall- oder Lebensversicherung oder einer privatärztlichen Verrechnungsstelle (§ 203 Abs. 1 Nr. 6 StGB)
- Gesetzliche Krankenkasse (§ 203 Abs. 2 StGB)
- Arzt, Zahnarzt, Tierarzt, Apotheker (§ 203 Abs. 1 Nr. 1 StGB)
- Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert (§ 203 Abs. 1 Nr. 1 StGB)

§ 203 StGB: Verarbeitung im Ausland

Verarbeitung im Ausland grundsätzlich erlaubt, ...

- Wortlaut von § 203 Abs. 3 S. 2 StGB steht einer Datentransferierung ins Ausland nicht entgegen
 - „[...] gegenüber sonstigen Personen offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist [...]“
- **Schutz der Geheimnisse muss aber auch im Ausland gewahrt bleiben, Schutzlücken dürfen nicht entstehen***
 - Im Gesetzesentwurf wurde zur Verdeutlichung bei den Berufsordnungen, die vom Bund geregelt werden, entsprechende Regelungen aufgenommen:
§ 43e Abs. 4 Bundesrechtsanwaltsordnung, § 39c Abs. 4 Patentanwaltsordnung § 62a Abs. 4 Steuerberatungsgesetz und § 50a Abs. 4 Wirtschaftsprüferordnung

* Gesetzesentwurf der Bundesregierung: Entwurf eines Gesetzes zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen. Drucksache 18/11936. online unter <https://dserver.bundestag.de/btd/18/119/1811936.pdf>

§ 203 StGB: Verarbeitung im Ausland

Verarbeitung im Ausland grundsätzlich erlaubt, aber Rechtslage ist zu prüfen

- Verarbeitung im Ausland grundsätzlich erlaubt
- Inanspruchnahme von Dienstleistungen, die im Ausland erbracht werden, nur möglich,
 - wenn der im Ausland bestehende Schutz der Geheimnisse dem Schutz im Inland vergleichbar
 - D.h. vor Beginn der Verarbeitung ist eine Prüfung des ausländischen Strafrechts erforderlich

§ 203 StGB: Verarbeitung im Ausland

Praxishilfe in Ausarbeitung

- Zum Thema § 203 StGB und Verarbeitung im Ausland ist eine Praxishilfe in Ausarbeitung
- Mit Themen wie
 - Berufsrecht – Datenschutzrecht – Strafrecht: Was regelt was?
 - Reichweite des § 203 StGB
 - § 203 StGB und die Verarbeitung durch Dienstleister im Ausland
 - Sanktionen bei einer unbefugten Offenbarung durch ausländische Dienstleister
 - Verschiedene Anhänge



Drittstaatentransfer

Cloud: Häufig kann eine Drittland-Verarbeitung nicht völlig ausgeschlossen werden

Definition eines Drittlands

- Keine Definition in Art. 4 DS-GVO („Begriffsbestimmungen“)
- Drittland (oder auch „Drittstaat“):
 - Staaten, die weder der EU angehören, noch zu den Staaten des EWR zählen
- Verarbeitung dort grundsätzlich erlaubt, aber
 - In diesen Staaten gilt anderes als europäisches Recht
 - Daher Verarbeitung dort nur unter bestimmten Voraussetzungen erlaubt

Verarbeitung personenbezogener Daten in einem Drittstaat

Allgemeine Voraussetzungen

- Grundsatz: Schutz personenbezogener Daten europäischer Bürger bleibt erhalten
- Verantwortlicher und Auftragsverarbeiter gewährleisten, dass
 - bei einer Verarbeitung in einem Drittland
 - oder einer Verarbeitung durch eine internationale Organisationdas durch die DS-GVO gewährleistete Schutzniveau für natürliche Personen vollumfänglich erhalten bleibt
- Verantwortlicher und/oder Auftragsverarbeiter in Drittland
 - Bestellen einen schriftlichen Vertreter (Art. 27 DS-GVO)
 - Vertreter ist in dem EU-Land, in dem sich Betroffene befinden, niedergelassen
 - Anlaufstelle für Aufsichtsbehörden und Betroffene

Verarbeitung personenbezogener Daten in einem Drittstaat

Vor Verarbeitungsbeginn im Drittland ist zu prüfen...

- Zwei Voraussetzungen müssen nach Art. 44 DS-GVO erfüllt sein:
 - 1) Die „sonstigen Bestimmungen dieser Verordnung“ müssen eingehalten werden
 - ➔ Insbesondere muss die Rechtmäßigkeit der Verarbeitung gewährleistet sein, d.h. ein Erlaubnistatbestand muss vorliegen (Artt. 6,9 DS-GVO)
 - 2) Vorgaben Kap. V (Art. 44ff DS-GVO) erfüllt, insbesondere
 - a) Feststellung angemessenes Schutzniveau durch EU-Kommission (Art. 45)
 - b) Datenübermittlung vorbehaltlich geeigneter Garantien (Art.46)
 - c) Verbindliche interne Datenschutzvorschriften (Art. 47)
 - d) Ausnahmen für bestimmte Fälle existieren (Art. 49)

Alle Instrumente **müssen** ein **dem EU-Datenschutzniveau angeglichenes Verhältnis im Drittland gewährleisten***

* Siehe auch Urteil EuGH in der Sache Schrems, AZ C-362/14. <https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A62014CJ0362>

Übermittlung an einen Empfänger

Kapitel V: Übermittlungen pbD an Drittländer oder an internationale Organisationen

- „transfer“: Alle Handlungen, durch welche ein Empfänger Kenntnis der pbD erhält
 - Empfänger im Sinne von Art. 4 Ziff. 9 DS-GVO, d.h. es spielt keine Rolle
 - ob Empfänger eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, ist oder
 - ob es sich um einen Dritten handelt oder nicht
 - Ausnahme entsprechend Art. 4 Ziff. 9 S. 2 DS-GVO:
 - Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags **nach dem Unionsrecht oder dem Recht der Mitgliedstaaten** möglicherweise personenbezogene Daten erhalten, sind keine Empfänger
 - Für Behörden in Drittländern i.d.R. nicht zutreffend!

EuGH in der Rechtssache C-311/18 (Schrems II)

Schutzniveau muss gewährleistet werden

- Rn. 83: Übermittlungen in Drittstaaten sind Verarbeitungen i.S.v. Art. 4 Nr. 2 DS-GVO, die DS-GVO findet Anwendung
- Rn. 87: Die etwaige Verarbeitung der betreffenden Daten durch ein Drittland für Zwecke der öffentlichen Sicherheit, der Landesverteidigung und der Sicherheit des Staates stellt die Anwendbarkeit der DSGVO auf die fragliche Übermittlung nicht in Frage.
- Rn. 92: Schutzniveau der DS-GVO muss bei Übermittlung gewährleistet werden
- ➔ Regelungen in Standardvertragsklauseln, BCR usw. müssen im Licht der Schrems II Urteils bewertet werden

Standarddatenschutzklauseln

Standarddatenschutzklauseln oder Standardvertragsklauseln?

- Art. 46 Abs. 2 lit. c DS-GVO: „**Standarddatenschutzklauseln**, die von der Kommission gemäß dem Prüfverfahren nach Artikel 93 Absatz 2 erlassen werden“
- Nutzung von der EU Kommission beschlossenen Vertragsklauseln: Keine Anzeigepflicht bei Aufsichtsbehörde
(„[...] ohne dass hierzu eine besondere Genehmigung einer Aufsichtsbehörde erforderlich wäre“)
 - Cave: Jede Abweichung von den Klauseln führt zur Anzeigepflicht!
- Ergänzungen sind i.d.R. keine Abweichung
 - ErwGr. 109: „[...] noch ihn daran hindern, ihnen weitere Klauseln oder zusätzliche Garantien hinzuzufügen, solange diese weder mittelbar noch unmittelbar im Widerspruch zu den von der Kommission oder einer Aufsichtsbehörde erlassenen Standard-Datenschutzklauseln stehen [...]“
- EU-Kommission nannte „Standarddatenschutzklauseln“ allerdings „Standardvertragsklauseln“
 - Klauseln online unter https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=de

Standardvertragsklauseln (standard contractual clauses, SCC)

Datenverkehr mit Drittstaaten

- Nutzung von Standardvertragsklauseln = Keine Genehmigung einer Aufsichtsbehörde erforderlich (Art. 46 Abs. 2 DS-GVO)
- ABER:
 - Selbstverständlich haben Aufsichtsbehörden ein Kontrollrecht, insbesondere haben sie auch das Recht, **Datenübermittlungen** zu **kontrollieren**
 - Auf Standardvertragsklauseln basierende **Übermittlungen** in ein Drittland **können** von Aufsichtsbehörde **ausgesetzt** oder auch **verboten werden**, wenn durch die Übermittlung EU- oder nationale Datenschutzvorschriften verletzt werden, beispielsweise wenn
 - der Datenimporteur die Standardvertragsklauseln missachtet,
 - der Datenimporteur sich weigert, mit den Datenschutzaufsichtsbehörden „redlich“ zusammenzuarbeiten oder
 - die Datenübermittlung sich wahrscheinlich negativ auf die Rechte betroffener Personen auswirkt.

Standardvertragsklauseln: Hinweis zu „Schrems II“

Schutzniveau der DS-GVO muss gewährleistet werden

- Werden personenbezogene Daten auf der Grundlage von Standarddatenschutzklauseln in ein Drittland übermittelt, so müssen diese den **Fortbestand des hohen Schutzniveaus sowohl bei der Übermittlung als auch bei der Verarbeitung in einem Drittland gewährleisten.**
- D. h. werden personenbezogene Daten auf der Grundlage von Standarddatenschutzklauseln in ein Drittland übermittelt, so muss ein Schutzniveau gewährleistet werden, das **dem in der Union garantierten Schutzniveau der Sache nach gleichwertig ist.**
- Bei der im Zusammenhang mit einer Drittland-Übermittlung erforderlichen Beurteilung sind insbesondere
 - die **vertraglichen Regelungen** zu berücksichtigen, die zwischen dem in der **Union ansässigen Verantwortlichen** bzw. seinem dort ansässigen **Auftragsverarbeiter** und dem im betreffenden **Drittland ansässigen Empfänger** der Übermittlung vereinbart wurden, sowie
 - die **maßgeblichen Elemente der Rechtsordnung dieses Landes**, soweit diese einen **etwaigen Zugriff der Behörden dieses Drittlands auf die übermittelten personenbezogenen Daten betreffen.**

Standardvertragsklauseln: Hinweis zu „Schrems II“

Schutzniveau der DS-GVO muss gewährleistet werden

- **Union ansässigen Verantwortlichen** bzw. dort ansässigen **Auftragsverarbeiters muss** insbesondere **geeignete Garantien vorsehen und prüfen**, ob durch diese Maßnahmen ein der DS-GVO **gleichwertiges Schutzniveau erreicht wird**
- **Kann** der in der Union ansässige Verantwortliche bzw. sein dort ansässiger Auftragsverarbeiter **keine hinreichenden zusätzlichen Maßnahmen ergreifen**, um einen solchen Schutz zu gewährleisten, ist er – bzw. in zweiter Linie die zuständige Aufsichtsbehörde – **verpflichtet**, die **Übermittlung** personenbezogener Daten **in das betreffende Drittland auszusetzen oder zu beenden**.
- Vertragsergänzungen beinhalten ein (nicht lösbares) Problem:
 - Auch die besten Vertragsklauseln können bei entsprechender Rechtslage im Drittland kein dem EU-Recht genügendes Datenschutzniveau etablieren

Drittstaatentransfer: Empfehlungen Europäischer Datenschutzausschuss

EDSA: „Empfehlungen 02/2020“

- EDSA veröffentlichte ebenfalls „Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen“ (Stand 2020-11-10)
https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_de
 - U.a. welche Anforderungen sind an die Rechtsordnung eines Drittstaates zu stellen, damit ein angemessenes Schutzniveau festgestellt werden kann

Drittstaatentransfer: Empfehlungen Europäischer Datenschutzausschuss

EDSA: „Empfehlungen 01/2020“

EDSA veröffentlichte „Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten“ (Stand 2021-06-18)

https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_de

- Empfehlungen bzgl. Vorgehen bei Drittlandtransfers
 1. Datentransfers identifizieren
 2. Wie erfolgt der Transfer? Welche Instrumente sind im Einsatz?
 3. Bewertung hinsichtlich Erfüllung Anforderungen Kap. V DS-GVO, insbesondere Art. 46
 4. Bei Bedarf: Festlegung ergänzender Maßnahmen zur Gewährleistung eines dem EU Recht entsprechenden Schutzniveaus
 5. Verfahrensschritte, zur Umsetzung der ergänzenden Maßnahmen
- Drei Anhänge, Anhang 1 enthält
 - ergänzende technische Maßnahmen (Verschlüsselung, Pseudonymisierung) und
 - die techn. Maßnahmen ggf. ergänzende vertragliche Regelungen

Beispiel: Mitbehandlung durch weisungsfreie Personen

Bewertung des Rechts des Drittstaates: Beispiel USA

- Schutz von Gesundheitsdaten
 - Health Insurance Portability and Accountability Act of (HIPAA)
 - 1996 eingeführt, 2003 durch Privacy Rule umgesetzt
 - Health Information Technology for Economic and Clinical Health Act (HITECH)
 - Praktische Durchsetzung von HIPAA gering
 - 2009 HITECH eingeführt, wodurch u.a. Geldstrafen bei Verstößen erhöht wurden
 - Zugleich Vertragspartner der Leistungserbringer direkt verpflichtet, d.h. neben Ärzte & Co werden auch Unternehmen in die Pflicht genommen
 - Gleichzeitig leichtere Nutzung von Daten zu Forschungszwecken ermöglicht
 - Genetic Information Nondiscrimination Act (GINA)
 - GINA ergänzt Privacy Rule bzgl. Umgang mit genetischen Daten
 - Schutzbereich nur für krankheitsrelevante Gesundheitsinformationen, Alter oder Geschlecht bspw. nicht geschützt
 - Forschung bzgl. Nutzung genetischer Informationen privilegiert

Beispiel: Mitbehandlung durch weisungsfreie Personen

Bewertung des Rechts des Drittstaates: Beispiel USA

- Schutz von Gesundheitsdaten
 - Landesrecht
 - Die meisten US Bundesstaaten erließen ergänzende Regelungen
 - Schutzniveau variiert daher erheblich von Bundesland zu Bundesland
 - Kritik
 - Keine einheitliche Interpretation
 - Schutzvorschriften gelten allerdings nach wie vor nicht für alle Formen der Gesundheitsversorgung und -forschung
 - Es existieren Widersprüche zu anderen gesetzlichen Regelungen
 - Aktuelle Regelungen wie der Coronavirus Aid, Relief, and Economic Security Act (CARES Act) schwächen die Schutzwirkung von HIPAA
 - Fazit:
 - Andere Zielrichtung der Gesetzgebung
 - Um ein der DS-GVO angemessenes Schutzniveau zu erzielen, müssen ergänzende vertragliche Vereinbarungen getroffen werden

Beispiel: Mitbehandlung durch weisungsfreie Personen

Bewertung des Rechts des Drittstaates: Beispiel USA

– Zugriff durch Behörden

Hinweis: Stark vereinfachte Darstellung

- 1) Natürlich müssen mehr Gesetze betrachtet werden und es
- 2) muss ein *angemessenes* Schutzniveau erzielt werden, kein *gleichwertiges*

➤ Auch mit vertraglichen Regelungen wird man ein dem EU-Recht entsprechendes Schutzniveau nicht erzielen können

Datenschutzkonferenz: Gutachten zum aktuellen Stand des US-Überwachungsrechts und der Überwachungsbefugnisse

DSK veröffentlichte Rechtsgutachten bzgl. Überwachungsbefugnisse in den USA

- DSK veröffentlichte am 25. Januar 2022 Rechtsgutachten bzgl. Überwachungsbefugnisse in den USA
 - Wesentliche Befunde des Gutachtens von Stephen I. Vladeck zur Rechtslage in den USA
https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/20220125_dsk_vladek.pdf
 - Gutachten zum aktuellen Stand des US-Überwachungsrechts und der Überwachungsbefugnisse (Deutsch)
https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladeck_Rechtsgutachten_DSK_de.pdf
 - Expert Opinion on the Current State of U.S. Surveillance Law and Authorities (English)
https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladeck_Rechtsgutachten_DSK_en.pdf
- Hinweis:
 - Prof. Stephen I Vladeck, Inhaber des Charles Alan Wright-Lehrstuhls für US-Bundesrecht an der University of Texas School of Law
<https://law.utexas.edu/faculty/stephen-i-vladeck>
 - Prof. Vladeck wurde von Facebook als Experte im Schrems-Verfahren hinzugezogen, Gutachten vom 2016-11-02 unter
https://iapp.org/media/pdf/resource_center/Schrems-testimony-Vladeck.pdf
- Originalgutachten in englischer Sprache, Kritik an der deutschen Übersetzung bei beck community
<https://community.beck.de/2022/02/09/die-deutsche-uebersetzung-des-gutachtens-von-herrn-stephen-vladeck>

Datenschutzkonferenz: Gutachten zum aktuellen Stand des US-Überwachungsrechts und der Überwachungsbefugnisse

DSK veröffentlichte Rechtsgutachten bzgl. Überwachungsbefugnisse in den USA

- Section 702 des FISA gilt für „Electronic Communication Service Provider“ im Sinne von 50 U.S. Code § 1881.
 - Dort findet sich in Absatz 4:
 - Electronic communication service provider
- The term “electronic communication service provider” means —
- a. a **telecommunications carrier**, as that term is defined in section 153 of title 47;
 - b. a **provider of electronic communication service**, as that term is defined in section 2510 of title 18;
 - c. a **provider of a remote computing service**, as that term is defined in section 2711 of title 18;
 - d. **any other communication service provider who has access to wire or electronic communications** either as such communications are transmitted or as such communications are stored; or
 - e. an officer, employee, or agent of an entity described in subparagraph (A), (B), (C), or (D).
- Insbesondere Anbieter von Cloud-Dienstleistungen, Anbieter von Cloud-Services fallen somit unter die Regelung

Datenschutzkonferenz: Gutachten zum aktuellen Stand des US-Überwachungsrechts und der Überwachungsbefugnisse

DSK veröffentlichte Rechtsgutachten bzgl. Überwachungsbefugnisse in den USA

- Gutachten-Ergebnisse zu Section 702 des US-amerikanischen Foreign Intelligence Surveillance Act (FISA) u.a.
 - Weiter Anwendungsbereich:
Neben den klassischen IT- und Telekommunikationsunternehmen können auch andere Unternehmen wie beispielsweise Banken oder Versanddienstleister in den Anwendungsbereich fallen
 - Es ist nicht erforderlich, dass der jeweilige Dienst öffentlich zur Verfügung steht. Vielmehr genügt es nach einem Gerichtsurteil, dass ein Unternehmen seinen Mitarbeitern einen entsprechenden Dienst (z.B. E-Mail-Dienst) bereitstellt, um in den Anwendungsbereich von FISA zu gelangen.
 - Alle Datenarten, auf die ein Unternehmen Zugriff hat, sind von FISA betroffen, nicht nur Kommunikationsdaten
 - Sofern sich Daten auf US-Servern befinden oder über eine US-Infrastruktur übertragen werden (können), können die Daten FISA unterfallen, unabhängig davon, wo sich das Unternehmen befindet, dem die Server und/oder Infrastruktur gehören.
 - Rechtsbehelfe gegen den Zugriff auf Daten betroffener EU-Bürger sind kaum verfügbar.

Cloud: Sicherheit der Verarbeitung

Cloud: Sicherheit der Verarbeitung

Technisch-organisatorische Maßnahmen

- Gesetzlich keine Cloud-spezifischen Vorgaben zur Sicherheit der Verarbeitung vorhanden
- Allgemeine Vorgaben aus DS-GVO, Bundes- und Landesrecht usw. sind natürlich auch bei Cloud-Einsatz zu beachten
 - DS-GVO: z.B. insbesondere Art. 25 Privacy by design/Default, Art. 32 Sicherheit der Verarbeitung, Art. 35 Datenschutz-Folgenabschätzung
 - Bundesrecht z.B.:
 - § 22 Abs. 2 BDSG
 - § 75b SGB V Sicherheit in der vertrags(zahn)ärztlichen Versorgung
 - § 75c SGB V IT-Sicherheit in Krankenhäusern
 - § 8a BSIG Sicherheit in der Informationstechnik Kritischer Infrastrukturen
 - Landesrecht i.d.R. keine über Bundesrecht hinausreichenden Vorgaben

Art. 25: Privacy by Design/Default

Wer muss sich darum kümmern?

- Normadressat
 - **Für die Daten Verantwortliche**, nicht Hersteller
- ErwGr. 78

„[...] sollten die Hersteller der Produkte, Dienste und Anwendungen ermutigt werden, das Recht auf Datenschutz bei der Entwicklung und Auslegung der Produkte, Dienste und Anwendungen zu berücksichtigen“
- Verantwortlicher darf (u.a.) nur Software einsetzen, die Tatbestand erfüllt
 - Keine Pflicht des Auftragsverarbeiters zur Unterstützung
 - Kundenservice?

Art. 25: Privacy by Design/Default

Anforderungen

- **Treffen geeigneter technisch-organisatorische Maßnahmen** (Art. 25 Abs. 2)
 - zur Umsetzung der Datenschutzgrundsätze
 - zur Durchsetzung der Betroffenenrechte
- unter Berücksichtigung (Art. 25 Abs. 1)
 - des Stands der Technik
 - der Implementierungskosten
 - der Art, Umfang, Umstände und Zwecke
 - der Eintrittswahrscheinlichkeiten und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen

Sicherheit der Verarbeitung (Art. 32 DS-GVO)

Technisch-organisatorische Maßnahmen (TOM) gefordert

Der **für die Verarbeitung Verantwortliche** und der **Auftragsverarbeiter** treffen unter Berücksichtigung

- des Stands der Technik,
- der Implementierungskosten und
- der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie
- der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die persönlichen Rechte und Freiheiten

geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (Art. 32 Abs. 1 DS-GVO)

Sicherheit der Verarbeitung (Art. 32 DS-GVO)

Angemessene Maßnahmen

Die Beurteilung der Angemessenheit ist eine Abwägung beinhaltend

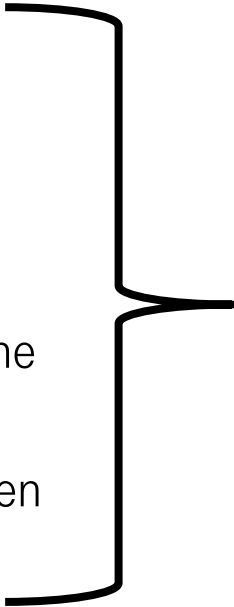
- Stand der Technik
- Implementierungskosten
- Art, Umfang, Umstände und Zwecke der Verarbeitung
- Eintrittswahrscheinlichkeit
- Schwere des Risikos für die persönlichen Rechte und Freiheiten

Technisch-organisatorische Maßnahmen (TOM)

Ziele der TOMs

Wahrung Datenschutzgrundsätze, d. h. per „Voreinstellung“ grundsätzlich nur Verarbeitung

- für den jeweiligen bestimmten Verarbeitungszweck
- nur die Menge an Daten und den Verarbeitungsumfang
- unter Beachtung der erforderliche Speicherfrist
- und wahren nur der erforderlichen Zugänglichkeit

- 
- Anforderungen von Art. 5 einhalten
 - Sicherheit der Verarbeitung gefordert

Technisch-organisatorische Maßnahmen (TOM)

Art. 32 Abs. 1 fordert...

- Maßnahmen u.a.
 - Pseudonymisierung
 - Verschlüsselung
- Fähigkeiten
 - Vertraulichkeit
 - Integrität
 - Verfügbarkeit
 - Belastbarkeit/Ausfallsicherheit
 - Wiederherstellbarkeit
 - Notfallmanagement
- Verfahren
 - Überprüfbarkeit
 - Bewertung
 - Evaluierung

Unter Berücksichtigung

- Stand der Technik
- Implementierungskosten
- Art, Umfang, Umstände und Zwecke der Verarbeitung
- Risiko der Verarbeitung

Technisch-organisatorische Maßnahmen (TOM)

TOM: Vorgabe durch Art. 32 Abs. 1 lit. a DS-GVO

- Risikoevaluierung und –beurteilung
- Darstellung eines Maßnahmenkatalogs
- (Interne) Audits inkl. Managementbewertung
- Verfahren zur Korrektur/Anpassung von ergriffenen Maßnahmen („PDCA-Zyklus“)
- Managementsystem inkl.
 - Datenschutzkonzept
 - IT-Sicherheitskonzept

Anforderungen Art. 25, 32 DS-GVO

Technisch-organisatorische Maßnahmen gefordert

- Art. 25 DS-GVO wie auch Art. 32 DS-GVO fordern technisch-organisatorische Maßnahmen, aber es gibt Unterschiede
 - Art. 25 DS-GVO
 - Trifft der Verantwortliche [...] **geeignete technische und organisatorische Maßnahmen** [...] die dafür ausgelegt sind, die **Datenschutzgrundsätze** [...] **wirksam umzusetzen** [...]
 - Art. 32 DS-GVO
 - Für die Verarbeitung Verantwortliche und der Auftragsverarbeiter treffen **geeignete technische und organisatorische Maßnahmen**, um ein dem Risiko **angemessenes** Schutzniveau zu gewährleisten
- Art. 25 DS-GVO enthält im Gegensatz zu Art. 32 DS-GVO keine Beschränkung bzgl. „Angemessenheit“ der Maßnahmen, Einhaltung Anforderungen Art. 5 ist zu gewährleisten

Cloud, TOM und Normen

Technisch-organisatorische Maßnahmen: Cloud und Normen

- Vertrag: ISO/IEC 19086 Rahmenwerk für Dienstgütevereinbarungen (SLA)
 - ISO/IEC 19086-1 (Stand: 2018-01) Übersicht und Konzepte
 - ISO/IEC 19086-2 (Stand: 2018-12) Metrisches Modell
 - ISO/IEC 19086-3 (Stand: 2017-07) Grundsätzliche Konformitätsanforderungen
 - ISO/IEC 19086-4 (Stand: 2019-01) Sicherheit und Datenschutz
- IT-Sicherheit
 - DIN EN ISO/IEC 27017 (Stand: 2021-11) Anwendungsleitfaden für Informationssicherheitsmaßnahmen basierend auf ISO/IEC 27002 für Cloud Dienste
 - DIN EN ISO/IEC 27018 (Stand: 2020-08) Leitfaden zum Schutz personenbezogener Daten (PII) in öffentlichen Cloud-Diensten als Auftragsdatenverarbeitung
 - ISO/IEC 27036-4 (Stand: 2016-10) Informationssicherheit für Zulieferbeziehungen - Teil 4: Leitlinien für die Sicherheit von Cloud-Diensten

Cloud, TOM und Normen

9 Zugangssteuerung

9.1 Geschäftsanforderungen an die Zugangsteuerung

Es gilt das Ziel von ISO/IEC 27002, 9.1.

9.1.1 Zugangssteuerungsrichtlinie

Es gelten die Maßnahme 9.1.1 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.

9.1.2 Zugang zu Netzwerken und Netzwerkdiensten

Es gelten die Maßnahme 9.1.2 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002. Außerdem gilt die folgende bereichsspezifische Anleitung.

E DIN EN ISO/IEC 27017:2020-09
prEN ISO/IEC 27017:2020 (D)

- Entwurf -

Anleitung zur Umsetzung für Cloud-Dienste

Cloud-Dienstleistungskunde	Cloud-Dienstleister
Die Zugangssteuerungsrichtlinie des Cloud-Dienstleistungskunden für die Nutzung von Netzwerken und Netzwerkdiensten sollte die Anforderungen an den Benutzerzugang für jeden einzelnen genutzten Cloud-Dienst festlegen.	(keine weitere Anleitung zur Umsetzung)

9.2 Benutzerzugangsverwaltung

Es gilt das Ziel von ISO/IEC 27002, 9.2.

9.2.1 Registrierung und Deregistrierung von Benutzern

Es gelten die Maßnahme 9.2.1 und die zugehörige Anleitung zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002. Außerdem gilt die folgende bereichsspezifische Anleitung.

Anleitung zur Umsetzung für Cloud-Dienste

Cloud-Dienstleistungskunde	Cloud-Dienstleister
(keine weitere Anleitung zur Umsetzung)	Um den Zugang zu Cloud-Diensten durch einen Cloud-Dienstleistungsnutzer des Cloud-Dienstleistungskunden zu verwalten, sollte der Cloud-Dienstleister dem Cloud-Dienstleistungskunden Funktionen für die Registrierung und Deregistrierung von Benutzern sowie Spezifikationen, wie diese Funktionen zu verwenden sind, bereitstellen.

Verweise auf ISO 27002

DEUTSCHE NORM **Entwurf** September 2020

DIN EN ISO/IEC 27017

ICS 03.100.70; 35.030 Einsprüche bis 2020-10-21

Entwurf

Informationstechnik –
Verfahren –
Leitfaden für Informationssicherheitsmaßnahmen basierend
auf ISO/IEC 27002 für Cloud Dienste (ISO/IEC 27017:2015);
und Englische Fassung prEN ISO/IEC 27017:2020

Information security –
Techniques –
Code of practice for information security controls based on ISO/IEC 27002 for cloud services
(ISO/IEC 27017:2015);
English version prEN ISO/IEC 27017:2020

Techniques de sécurité –
Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002
pour les services du nuage (ISO/IEC 27017:2015);
Version allemande et anglaise prEN ISO/IEC 27017:2020

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2020-08-21 wird der Öffentlichkeit zur Prüfung und
Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs
besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwurf bzw. für Norm-
Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwurfe.normenbibliothek.de,
sofern dort wiedergegeben;
- oder als Datei per E-Mail an nia@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im
Internet unter www.din.de/go/stellungnahmen-norm-entwurf oder für Stellungnahmen zu Norm-
Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA),
10772 Berlin oder Saatwinkler Damm 42/43, 13627 Berlin.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten
Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 96 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

© DIN Deutsches Institut für Normung e. V. ist Inhaber aller einfallenden Rechte der Verwertung, gleich in
welcher Form und welchem Verfahren.
Alleinverkauf durch Beuth Verlag GmbH, 10772 Berlin www.din.de
www.beuth.de

3181014



HEALTHCARE SOLUTIONS

Literaturhinweise

> ISO/IEC 27017:2015(E)

- Entwurf -

Cloud, TOM und Normen

10 Kryptographie

10.1 Kryptographische Maßnahmen

Es gilt das in ISO/IEC 27002:2013, 10.1, festgelegte Ziel.

10.1.1 Richtlinie zum Gebrauch von kryptographischen Maßnahmen

Es gelten die Maßnahme 10.1.1 und die zugehörigen Anleitungen zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002. Außerdem gilt die folgende bereichsspezifische Anleitung.

Verweise auf ISO 27002

DIN EN ISO/IEC 27018:2020-08
EN ISO/IEC 27018:2020 (D)

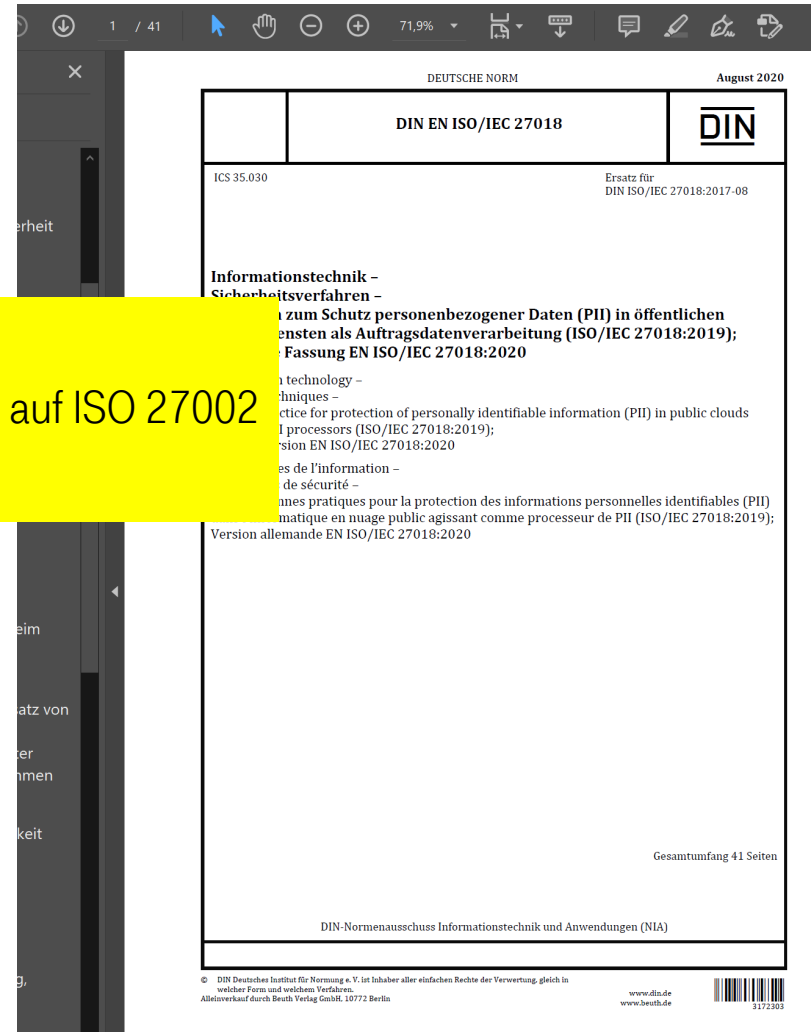
Anleitung für die Umsetzung von Datenschutzmaßnahmen bei Public-Cloud-Anwendungen

Der Public-Cloud-Auftragsdatenverarbeiter sollte dem Cloud-Dienstleistungskunden Informationen zu den Umständen zur Verfügung stellen, unter denen er kryptographische Mittel anwendet, um die von ihm verarbeiteten pD zu schützen. Der Public-Cloud-Auftragsdatenverarbeiter sollte dem Cloud-Dienstleistungskunden außerdem Informationen zu den von ihm bereitgestellten Kapazitäten zur Verfügung stellen, die dem Cloud-Dienstleistungskunden bei der Anwendung seiner eigenen kryptographischen Schutzmaßnahmen helfen können.

ANMERKUNG Einige Rechtssysteme können die Anwendung von kryptographischen Verfahren zum Schutz bestimmter Arten von pD verlangen, wie z. B. Gesundheitsdaten von Betroffenen, Einwohnermeldenummern, Passnummern und Führerscheinnummern.

10.1.2 Schlüsselverwaltung

Es gelten die Maßnahme 10.1.2 und die zugehörigen Anleitungen zur Umsetzung sowie die weiteren Informationen nach ISO/IEC 27002.



Cloud, TOM und Normen

DIN EN ISO/IEC 27701 ergänzt, Anhang E beachten

DEUTSCHE NORM Juli 2021

	DIN EN ISO/IEC 27701	DIN
--	-----------------------------	------------

ICS 35.030

**Sicherheitstechniken -
Erweiterung zu ISO/IEC 27001 und ISO/IEC 27002 für das Management
von Informationen zum Datenschutz -
Anforderungen und Leitlinien (ISO/IEC 27701:2019);
Deutsche Fassung EN ISO/IEC 27701:2021**

Security techniques -
Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management -
Requirements and guidelines (ISO/IEC 27701:2019);
German version EN ISO/IEC 27701:2021

Techniques de sécurité -
Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection
de la vie privée -
Exigences et lignes directrices (ISO/IEC 27701:2019);
Version allemande EN ISO/IEC 27701:2021

Gesamtumfang 88 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

© DIN Deutsches Institut für Normung e. V. ist Inhaber aller einfachen Rechte der Verwertung, gleich in
welcher Form und welchem Verfahren. www.din.de
Alleinverkauf durch Beuth Verlag GmbH, 10772 Berlin www.beuth.de

DIN EN ISO/IEC 27701:2021-07
EN ISO/IEC 27701:2021 (D)

Anhang E
(informativ)

Zuordnung zu ISO/IEC 27018 und ISO/IEC 29151

ISO/IEC 27018 enthält weitere Informationen für Organisationen, die als Auftragsverarbeiter tätig sind und öffentliche Cloud-Dienste anbieten. ISO/IEC 29151 enthält zusätzliche Maßnahmen und Leitlinien für die Verarbeitung von personenbezogenen Daten durch verantwortliche Stellen.

Tabelle E.1 gibt eine indikative Zuordnung zwischen den Bestimmungen dieses Dokuments und den Datenschutzprinzipien aus ISO/IEC 27018 und ISO/IEC 29151. Sie zeigt, wie die Anforderungen und Maßnahmen dieses Dokuments in gewisser Weise mit den Bestimmungen von ISO/IEC 27018 und/oder ISO/IEC 29151 übereinstimmen können.

Sie ist rein indikativ und es sollte nicht angenommen werden, dass eine bestimmte Verbindung zwischen den Bestimmungen Gleichwertigkeit bedeutet.

Tabelle E.1 — Zuordnung der ISO/IEC 27701 auf ISO/IEC 27018 und ISO/IEC 29151

Unterschnitt in diesem Dokument	Unterschnitt in ISO/IEC 27018	Unterschnitt in ISO/IEC 29151
5.2	entfällt	entfällt
5.3	entfällt	entfällt
5.4	entfällt	4.2
5.5	entfällt	7.2.3
5.6	entfällt	entfällt
5.7	entfällt	entfällt
5.8	entfällt	entfällt
6.1	entfällt	entfällt
6.2	5.1.1	5
6.3	6.1.1	entfällt
6.4	7.2.2	entfällt
6.5.1	entfällt	8.1
6.5.2	entfällt	8.2
6.5.3	A.11.4, A.11.5	8.3
6.6.1	entfällt	entfällt
6.6.2	9.2.1, A.11.8, A.11.9, A.11.10	9.2
6.6.3	entfällt	9.3
6.6.4	7.2.2, 9.4.2	9.4
6.7	10.1.1	entfällt
6.8.1	entfällt	11.1
6.8.2	11.2.7, A.11.2, A.11.13	entfällt



Sicherheit der Verarbeitung in der Cloud: BSI

Technisch-organisatorische Maßnahmen: BSI

- Mindeststandard des BSI nach § 8 Abs. 1 Satz 1 BSIg zur Nutzung externer Cloud-Dienste in der Bundesverwaltung

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_Nutzung_externer_Cloud-Dienste.html

- Referenztable:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Referenztable_Mindeststandard_externe_Cloud-Dienste_V2_0-Grundsutz2021.html

- Umsetzungshinweise:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Umsetzungshinweise_Mindeststandards_Externe_Cloud-Dienste.html

- FAQ

https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/FAQ_MST_Externe_Cloud-Dienste/faq_mst_Externe_Cloud-Dienste_node.html

Sicherheit der Verarbeitung in der Cloud: BSI

Technisch-organisatorische

- Mindeststandards für Cloud-Dienste in der BSI

NCD.2.2.03 Gerichtsbarkeit vertraglich zusichern

- Die Einrichtung SOLLTE zur Absicherung der Verfügbarkeit als Teil der Informationssicherheit Vereinbarungen ausschließlich nach deutschem Recht und deutschem Gerichtsstand und ohne obligatorisch vorab zu betreibende Schlichtungsverfahren abschließen.
- Die Einrichtung MUSS berücksichtigen, dass bei gegebenenfalls notwendigem Rechtsschutz beziehungsweise Eilrechtsschutz Zeitverluste eintreten können, insbesondere durch eine Einarbeitung in fremde Rechtsordnungen oder ein Auftreten vor entfernt gelegenen Gerichten.
- Die Einrichtung MUSS beim Verhandeln des Vertrages sicherstellen, dass sie handlungsfähig bleibt und ihre Forderungen effektiv durchsetzen kann.

NCD.2.2.04 Lokation vertraglich zusichern

- Die Einrichtung MUSS prüfen, ob die dienstlichen Daten an den vertraglich zugesicherten Lokationen verarbeitet werden dürfen. Hierzu MUSS die Einrichtung die Ergebnisse der Datenkategorisierung und der Risikoanalyse, das mögliche Risiko eines fremdstaatlichen Zugriffs (z. B. durch Nachrichtendienste oder

³² Kriterienkatalog Cloud Computing (C5:2020), (BSI 2020a), Kap. 4.4.5, S.18f.

2 Sicherheitsanforderungen

Ermittlungsbehörden) sowie weitere Anforderungen (z. B. aus Gesetzen, Verordnungen, Beschlüssen oder anderen Quellen) bewerten.

- Die Einrichtung MUSS sämtliche Lokationen, an denen der Cloud-Diensteanbieter mit dem Cloud-Dienst dienstliche Daten speichert und verarbeitet, vertraglich festlegen. Dabei MUSS die Einrichtung auch Datensicherungen berücksichtigen, da diese ggf. an Drittlukationen durchgeführt werden.

NCD.2.2.05 Offenbarungspflichten und Ermittlungsbefugnisse vertraglich zusichern

- Die Einrichtung MUSS die Pflichten des Cloud-Diensteanbieters, sicherheitsrelevante Vorfälle (sowie ggf. andere Vorfälle) gegenüber der Einrichtung zu melden, vertraglich regeln.
 - Die Einrichtung MUSS beim Festlegen von Vertragsstrafen und Haftungsfragen auf ein angemessenes Verhältnis zum ermittelten Schutzbedarf der mit dem Cloud-Dienst verarbeiteten dienstlichen Daten achten.
 - Beim Festlegen von Vertragsstrafen und Haftungsregelungen sind die aus rechtlicher Sicht zulässigen Grenzen zu berücksichtigen. Die Einrichtung SOLLTE bei der Ansetzung von Vertragsstrafen 5% des Auftragsvolumens nicht unterschreiten.

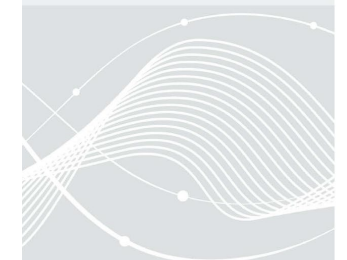
Öffentlicher Cloud-



Deutschland
Digital•Sicher•BSI

Leitlinie des BSI zur Sicherheit von Cloud-Diensten

Version 2.0 vom 07.07.2021



Sicherheit der Verarbeitung in der Cloud: BSI

NCD.2.2.03 Gerichtsbarkeit vertraglich zusichern

a) Die Einrichtung SOLLTE zur Absicherung der Verfügbarkeit als Teil der Informationssicherheit Vereinbarungen ausschließlich nach deutschem Recht und deutschem Gerichtsstand und ohne obligatorisch vorab zu betreibende Schlichtungsverfahren abschließen.

b) Die Einrichtung MUSS berücksichtigen, dass bei gegebenenfalls notwendigem Rechtsschutz beziehungsweise Eilrechtsschutz Zeitverluste eintreten können, insbesondere durch eine Einarbeitung in fremde Rechtsordnungen oder ein Auftreten vor entfernt gelegenen Gerichten.

c) Die Einrichtung MUSS beim Verhandeln des Vertrages sicherstellen, dass sie handlungsfähig bleibt und ihre Forderungen effektiv durchsetzen kann.

Vor dem Hintergrund des jeweiligen Anwendungsfalles ist zu prüfen, welche Bedeutung ein Gerichtsstand außerhalb von Deutschland hätte. Hierbei ist insbesondere zu bewerten, inwiefern Durchsetzungsrechte oder Eilrechtsschutz von Bedeutung sind. Gleiches gilt für das anzuwendende Recht.

Liegt ein Prüfbericht nach C5:2020 vor, können diese Angaben der Rahmenbedingung „BC-01 Angaben zu Gerichtsbarkeit und Lokationen“ bzw. nach C5:2016 dem Umfeldparameter „UP-02 Gerichtsbarkeit und

Bundesamt für Sicherheit in der Informationstechnik

21

2 Umsetzungshinweise zu den Sicherheitsanforderungen

Lokationen der Datenspeicherung, -verarbeitung und -sicherung“ entnommen werden. Sie sind daher im Prüfbericht nach C5 zu finden.

Eine Bewertung des anwendbaren Rechts könnte aufgeteilt nach Regionen erfolgen:

- Deutsches Recht,
- Recht eines EU-Mitgliedstaates,
- Recht eines Nicht-EU-Mitgliedstaates.

Kommt es zu einer gerichtlichen Auseinandersetzung nimmt der Gerichtsstand eine wichtige Rolle ein. Vor diesem Hintergrund könnte die Zuordnung des Gerichtsstandes nach Regionen erfolgen:

- Deutschland,
- EU-Mitgliedsstaat,
- Nicht EU-Mitgliedsstaat.

NCD.2.2.04 Lokation vertraglich zusichern

Technisch-organisatorische

- Mindeststandard für Cloud-Dienste in der Bundesrepublik

aner Cloud-



Deutschland
Digital•Sicher•BSI

weise zum
des BSI zur
Cloud-Dienste 2.0

Sicherheit der Verarbeitung in der Cloud: BSI

Technisch-organisatorische Maßnahmen: BSI

- BSI adressiert Cloud Computing natürlich auch im IT-Grundschutz:
- Baustein OPS.2.2 Cloud-Nutzung (Edition 2022)
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompodium_Einzel_PDFs_2022/04_OPS_Betrieb/OPS_2_2_Cloud-Nutzung_Edition_2022.html
 - Basis-Maßnahmen, z.B.
 - Erstellung einer Cloud-Nutzungs-Strategie
 - Standard-Maßnahmen, z.B.
 - Planung der sicheren Einbindung von Cloud-Diensten
 - Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung
 - Maßnahmen für erhöhten Schutzbedarf
 - Durchführung eigener Datensicherungen
 - Einsatz von Verschlüsselung bei Cloud-Nutzung

Sicherheit der Verarbeitung in der Cloud: BSI

Technisch-organisatorische Maßnahmen: BSI

- BSI adressiert Cloud Computing natürlich auch im IT-Grundschutz Baustein OPS.2.2 Cloud-Nutzung (Edition 2022)

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein OPS.2.2 *Cloud-Nutzung* exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse.

OPS.2.2.A15 Sicherstellung der Portabilität von Cloud-Diensten [Fachverantwortliche] (H)

Der Cloud-Kunde SOLLTE alle Anforderungen definieren, die es ermöglichen, einen Cloud-Diensteanbieter zu wechseln oder den Cloud-Dienst bzw. die Daten in die eigene IT-Infrastruktur zurückzuholen. Zudem SOLLTE der Cloud-Kunde regelmäßig Portabilitätstests durchführen. Im Vertrag mit dem Cloud-Diensteanbieter SOLLTEN Vorgaben festgehalten werden, mit denen sich die notwendige Portabilität gewährleisten lässt.

OPS.2.2.A16 Durchführung eigener Datensicherungen [Fachverantwortliche] (H)

Der Cloud-Kunde SOLLTE prüfen, ob, zusätzlich zu den vertraglich festgelegten Datensicherungen des Cloud-Diensteanbieters, eigene Datensicherungen erstellt werden sollen. Zudem SOLLTE er detaillierte Anforderungen an einen Backup-Service erstellen.



OPS.2.2 Cloud-Nutzung

1. Beschreibung

1.1. Einleitung

Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannweite der im Rahmen von Cloud Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Software.

Cloud Computing bietet viele Vorteile. Die IT-Dienste können bedarfsgerecht, skalierbar und flexibel genutzt und je nach Funktionsumfang, Nutzungsdauer und Anzahl der Benutzer abgerechnet werden. Auch kann auf spezialisierte Kenntnisse und Ressourcen des Cloud-Diensteanbieters zugegriffen werden, wodurch interne Ressourcen für andere Aufgaben freigesetzt werden können. In der Praxis zeigt sich jedoch häufig, dass sich die Vorteile, die Institutionen von der Cloud-Nutzung erwarten, nicht vollständig auswirken. Die Ursache dafür ist meistens, dass wichtige kritische Erfolgsfaktoren im Vorfeld der Cloud-Nutzung nicht ausreichend betrachtet werden. Daher müssen Cloud-Dienste strategisch geplant sowie (Sicherheits-)Anforderungen, Verantwortlichkeiten und Schnittstellen sorgfältig definiert und vereinbart werden. Auch das Bewusstsein und Verständnis für die notwendigerweise geänderten Rollen, sowohl auf Seiten des IT-Betriebs als auch der Benutzer der nutzenden Institution, ist ein wichtiger Erfolgsfaktor.

Zusätzlich sollte bei der Einführung von Cloud-Diensten auch das Thema Governance berücksichtigt werden (Cloud Governance). Kritische Bereiche sind beispielsweise die Vertragsgestaltung, die Umsetzung von Mandantenfähigkeit, die Sicherstellung von Portabilität unterschiedlicher Services, die Abrechnung genutzter Service-Leistungen, das Monitoring der Service-Erbringung, das Sicherheitsvorfallmanagement und zahlreiche Datenschutzaspekte.

1.2. Zielsetzung

Der Baustein beschreibt Anforderungen, durch die sich Cloud-Dienste sicher nutzen lassen. Er richtet sich an alle Institutionen, die solche Dienste bereits nutzen oder sie zukünftig einsetzen wollen.

1.3. Abgrenzung und Modellierung

Der Baustein OPS.2.2 *Cloud-Nutzung* ist immer auf eine konkrete Cloud-Dienstleistung anzuwenden. Nutzt eine Institution unterschiedliche Cloud-Diensteanbieter, so ist der Baustein für jeden Cloud-Diensteanbieter einmal anzuwenden. Die Schnittstelle zwischen den Cloud-Diensteanbietern ist ebenfalls Gegenstand des Bausteins und muss für alle Cloud-Dienstleistungen betrachtet werden.

- 2.9. Unzureichende Regelungen für das Ende eines Cloud-Nutzungs-Vorhabens
- 2.10. Unzureichendes Administrationsmodell für die Cloud-Nutzung
- 2.11. Unzureichendes Notfallvorsorgekonzept
- 2.12. Ausfall der IT-Systeme eines Cloud-Diensteanbieters
- 3. Anforderungen
 - 3.1. Basis-Anforderungen

Sicherheit der Verarbeitung in der Cloud: BSI

Technisch-organisatorische Maßnahmen: BSI

- BSI entwickelte 2016 Kriterienkatalog C5 (Cloud Computing Compliance Criteria Catalogue)
- Aktuelle Version C5:2020
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/C5_AktuelleVersion/C5_AktuelleVersion_node.html
- Mindestanforderungen an IT-Sicherheit für Cloud Computing
- Kriterienkatalog bietet Möglichkeit, dass sich Cloud-Anbieter Einhaltung bestätigen lassen
- Mappingtabelle zu internationalen Standards inkl. ISO/IEC 27017
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CloudComputing/Anforderungskatalog/2020/C5_2020_Referenztable.xlsx?__blob=publicationFile&v=1

Sicherheit und Cloud: Die europäische Sicht - ENISA

Agentur der Europäischen Union für Cybersicherheit (ENISA): Cloud Security

- European Cybersecurity Certification Scheme (EUCCS) for Cloud Services
 - <https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme>
 - Stand: 2020-12-22
 - Draft zur Zertifizierung der Cybersicherheit von Cloud-Diensten
- Cloud Security for Healthcare Services
 - <https://www.enisa.europa.eu/publications/cloud-security-for-healthcare-services>
 - Stand: 2021-01-18
 - Studie mit dem Ziel
 - Sicherheitsaspekte, einschließlich relevanter Datenschutzaspekte, bei Cloud-Nutzung zu identifizieren
 - Identifizierung relevanter Bedrohungen und Risiken für Cloud-Dienste im Gesundheitswesen
 - Betrachtung von Anforderungen an Sicherheit und Datenschutz
 - Unterstützung bei der Auswahl geeigneter technischer und organisatorischer Maßnahmen

Sicherheit und Cloud: Die europäische Sicht - ENISA

Agentur der Europäischen Union für Cybersicherheit (ENISA): Cloud Security

– Securing Cloud Services for Health

<https://www.enisa.europa.eu/news/enisa-news/securing-cloud-services-for-health>

- Stand: 2021-01-18
- Betrachtung von Cybersicherheitsrisiken bei der Nutzung von Cloud-Diensten
- Cybersicherheitsleitlinien für Gesundheitsorganisationen für 3 Einsatzszenarien:
 - Elektronische Gesundheitsakten (EPA)
 - Telemedizin, genauer Fernkonsultation bei Arzt-Patienten Kommunikation
 - Einbindung von Medizinprodukten bzw. Integration der dort anfallenden Patientendaten in der Cloud

Sicherheit und Cloud: Code of Conduct

Keine anerkannten Verhaltensregeln für Deutschland

- Stand heute existierten keine Verhaltensregeln bzgl. Nutzung von Cloud Computing, die
 - entweder von einer deutschen Aufsichtsbehörde
 - oder von EDSA*
anerkannt wurden
- Verschiedentlich wird auf von Scope entwickelten „EU Cloud Code of Conduct“ verwiesen
<https://eucoc.cloud/en/about/about-eu-cloud-coc/>
 - Auch dieser CoC stellt keine für Deutschland geltenden anerkannten Verhaltensregeln entsprechend Art. 40 DS-GVO dar
 - Unabhängig davon spricht nichts dagegen, diesen CoC zu nutzen, wenn er passt
- Gleiches gilt für auch andere wie beispielsweise dem französischen CISPE-Ansatz
 - EDSA-Opinion zu CISPE unter
https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-172021-draft-decision-french-supervisory_en

* Von EDSA anerkannte CoC online unter

https://edpb.europa.eu/our-work-tools/accountability-tools/register-codes-conduct-amendments-and-extensions-art-4011_de

Sicherheit und Cloud: Zertifizierung

Zertifizierung möglich, aber keine entsprechend Art. 42 DS-GVO

- Vorab: es gibt Stand heute keine Zertifizierung entsprechend Art. 42 DS-GVO
- Aber einige Zertifizierungen, z.B.
 - Zertifizierung nach DIN EN ISO/IEC 27017
(nur in Verbindung mit Zertifizierung nach ISO 27001)
 - Andere Zertifizierungen wie beispielsweise EuroPriSe
(<https://www.euprivacyseal.com/>) sind allgemeiner Natur, können aber auch Cloud-Dienstleistungen abbilden und dementsprechend zertifizieren
- In Deutschland sehr anerkannt: Gütesiegel „Trusted Cloud“

Sicherheit und Cloud: Zertifizierung

Zertifizierung möglich, aber keine entsprechend Art. 42 DS-GVO

- 2015 wurde Verein „Kompetenznetzwerk Trusted Cloud e. V.“ gegründet (aus Technologieprogramm des BMWi hervorgegangen)
- Webseite Verein: <https://trusted-cloud.de/>
- Verein entwickelte Gütesiegel für vertrauenswürdige Cloud Services
 - (Pilot)Zertifizierungen nach „AUDITOR“
<https://www.auditor-cert.de/>
 - Projekt Veröffentlichungen unter <https://www.auditor-cert.de/publikationen/>
 - Kriterienkatalog v0.99 online
<https://www.auditor-cert.de/kb/kriterienkatalog/>
 - Akkreditierung durch DAkkS angestrebt sollte Sommer 2020 abgeschlossen sein; allerdings bis heute nicht erfolgt
 - In Entwicklung:
Trusted Cloud Datenschutz-Profil für Cloud-Dienste (TCDP)
<https://www.tcdp.de/>
→ Prüfstandard für datenschutzrechtliche Anforderungen

Sicherheit und Cloud: Herausforderungen

Worüber man sich auch Gedanken machen sollte

- Intrusion Detection
 - Vorgaben insbesondere auch für KRITIS-Strukturen
 - In Cloud häufig nur mit Cloud-Provider möglich
- Digitale Forensik
 - Bei Sicherheitsvorfällen ist i.d.R. eine Untersuchung erforderlich
 - Beweissicherung auf „normalen“ IT-Systemen erfordert Fachkenntnis bzgl. digitaler Forensik
 - Digitale Forensik in der Cloud noch einmal andere Hausnummer
 - Unversehrtheit des Beweismittels
 - Zeitdruck: Logdateien werden beispielsweise überschrieben
 - Kooperation des Cloud-Providers

Sicherheit und Cloud: Herausforderungen

Worüber man sich auch Gedanken machen sollte

- Audits
 - Auditoren (z.B. ISO 27001, aber auch QM-Audits) fragen regelhaft nach Prüfung von Zugriffen, d.h. Nutzung von Protokolldateien
 - Innerhalb durch von Cloud-Provider bereitgestellte VM: I.d.R. voller Zugriff
 - Manipulationen der VM kann so häufig nicht erkannt werden:
Wie wird gegenüber Auditoren die Sicherheit der VM sowie die Kontrolle nachgewiesen
- Haftungsfragen
 - Cloud Provider schließen Haftung für sich selbst weitestgehend aus
 - Haftung gegenüber betroffener Person bleibt bestehen, Regelung zwischen Cloud-Provider und Auftraggeber kann nur Innenverhältnis betreffen
 - Daher Prüfung erforderlich, welche Folgen Outsourcing hier ggf. bedeutet

Dokumentationspflichten

Dokumentationspflicht inkl. Auditierung

DS-GVO verpflichtet zur Dokumentation sowie zur Prüfung der DS-GVO-Einhaltung

- Art. 5 Abs. 2 DS-GVO
Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen **Einhaltung nachweisen**
- Art. 24 DS-GVO
Verantwortliche setzt technische und organisatorische Maßnahmen zum Schutz der von der Verarbeitung betroffenen Person um; diese **Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.**
- Dies gilt selbstverständlich auch bei Nutzung einer Cloud

Rechenschaftspflicht nach Art. 5 DS-GVO

Verantwortliche muss nachweisen

- Rechtmäßigkeit
- Transparenz (inkl. Drittland-Verarbeitung)
- Verantwortlicher
- Zweck(e) / Zweckbindung
- Datenminimierung
- Richtigkeit
- Betroffene (Kategorien)
- Daten (Kategorien)
- Empfänger (Kategorien)
- Löschfristen / Speicherbegrenzung
- Integrität, Vertraulichkeit

Nachweis der Einhaltung der Vorgaben bzgl. Privacy by Design/Default

Privacy by Design/Default betrifft vollständigen Daten-Lebenszyklus

- Art. 25 Abs. 1 DS-GVO
[...] trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen [...]
- Zielsetzung (Art. 25 Abs. 1 DS-GVO)
[...] die Datenschutzgrundsätze [...] wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen
- **Anforderung zur Dokumentation ergibt sich indirekt aus Art. 25 Abs. 3 DS-GVO**

Cloud i.d.R. Auftragsverarbeitung

Vertrag zur Auftragsverarbeitung muss existieren

- Verantwortlicher muss nachweisen
 - Kriterien für die Auswahl des Auftragsverarbeiters
 - Einhaltung Vorgaben Art. 32 DS-GVO (Sicherheit Verarbeitung)
 - Gewährleistung der Rechte der betroffenen Person
 - Durchführung und das Ergebnis einer Vor-Ort-Prüfung (wenn durchgeführt)
 - Einhaltung Vertragspflichten
 - Nachweis muss für gesamte Dauer der Verarbeitung geführt werden
- Pflicht zum Vertragsabschluss (schriftlich)
 - Inhaltliche Vorgaben aus Art. 28 Abs. 3 S. 2 lit. a-h DS-GVO (siehe auch Muster-Vertrag zur Auftragsverarbeitung für das Gesundheitswesen*)
 - Weitere Vorgaben bzgl. Verarbeitung im Auftrag nicht zwingend Vertragsbestandteil, muss aber ggf. nachgewiesen werden, z.B.
 - Nicht in der Union niedergelassene Verantwortlichen oder Auftragsverarbeitern benötigen Vertreter in der Union
 - Artt. 44ff DS-GVO: Verarbeitung in Drittstaaten

* Mustervertrag zur Auftragsverarbeitung, online unter <http://ds-gvo.gesundheitsdatenschutz.org/html/adv-vertrag.php>

Sicherheit der Verarbeitung (Art. 32 DS-GV)

Sicherheit der Verarbeitung muss nachgewiesen werden

- Verantwortliche und der Auftragsverarbeiter setzen geeignete technische und organisatorische Maßnahmen ein, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:
 - Pseudonymisierung und Verschlüsselung personenbezogener Daten
 - Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste auf Dauer sicherzustellen;
 - die Verfügbarkeit und Zugang der Daten bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
 - Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOMs
- **Nachweis der Maßnahmen erforderlich
(indirekte Pflicht resultierend aus Art. 32 Abs. 3 DS-GVO)**

Dokumentation bei Drittlandverarbeitung

Dokumentation nicht direkt erforderlich, aber ...

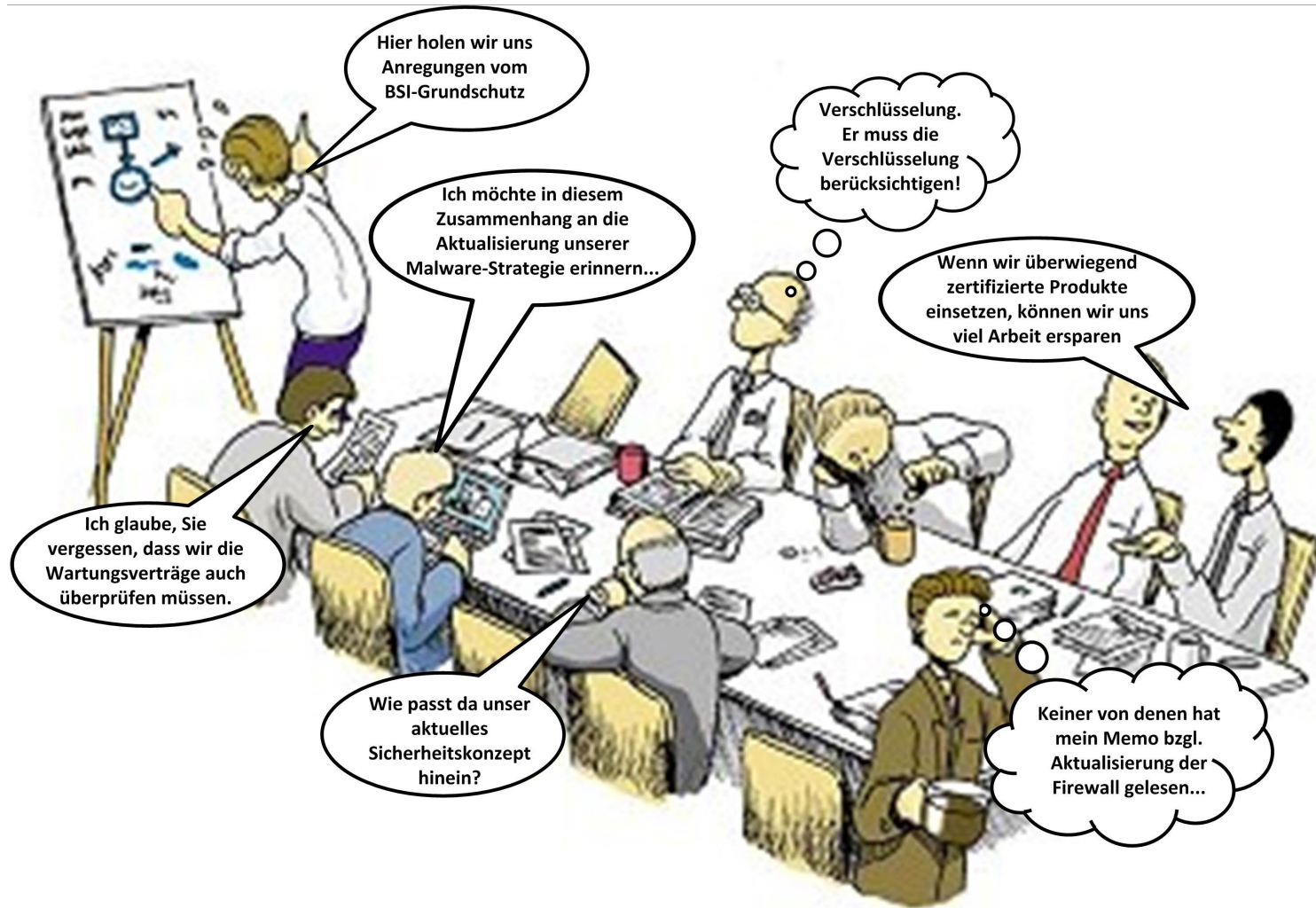
- Art. 44 DS-GVO
[...] ist nur zulässig, wenn der Verantwortliche und der Auftragsverarbeiter die in diesem Kapitel niedergelegten Bedingungen einhalten und auch die sonstigen Bestimmungen dieser Verordnung eingehalten werden; [...]
- Insbesondere gilt auch die Nachweispflicht aus Art. 5 DS-GVO (Accountability)
- Art. 44 DS-GVO
Alle Bestimmungen dieses Kapitels sind anzuwenden, um sicherzustellen, dass das durch diese Verordnung gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird.
- **Es ist ein Nachweis erforderlich, wie das Schutzniveau erhalten bleibt**

Datenschutz-Folgenabschätzung bei Cloud wahrscheinlich erforderlich

Dokumentation muss nach Art. 35 DS-GVO mindestens enthalten

- Rechtmäßigkeit
- Systematische Beschreibung der geplanten Verarbeitungsvorgänge; dies beinhaltet u.a.
 - Betroffene (Kategorien)
 - Daten (Kategorien)
 - Empfänger (Kategorien)
 - Löschfristen
 - Drittland-Verarbeitung
- Zwecke der Verarbeitung
- Ggf. die vom Verantwortlichen verfolgten berechtigten Interessen
- Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck
- Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen
- Zur Bewältigung der Risiken geplanten Abhilfemaßnahmen („TOM“)
- Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird

Diskussion / Fragen



Kontakt: Bernd.Schuetze@T-Systems.com



HEALTHCARE SOLUTIONS