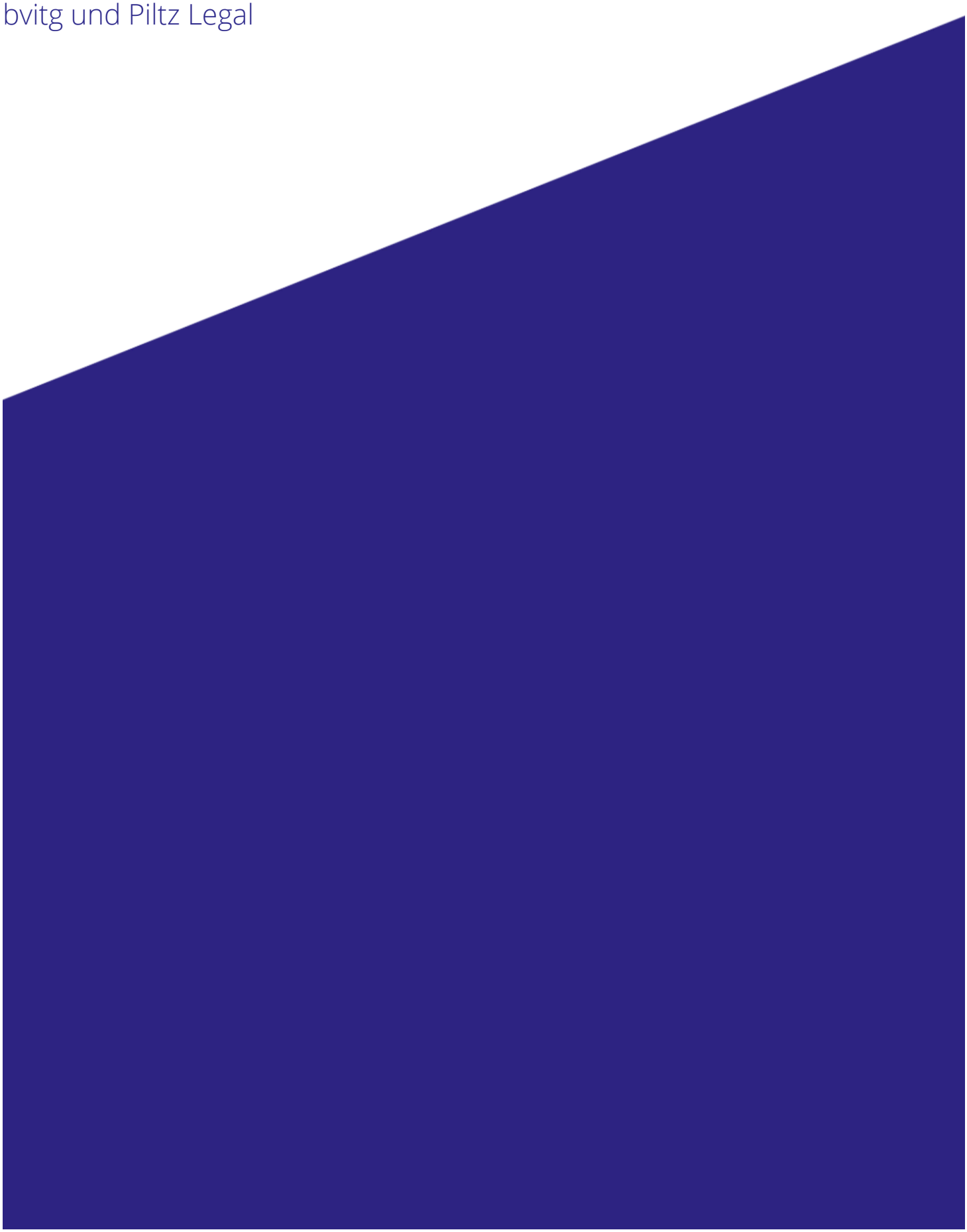
FAQ zum Gutachten in Bezug auf Vorgaben aus § 393 SGB V

bvitg und Piltz Legal



30 Jahre bvitg

Piltz Legal

Der Bundesverband Gesundheits-IT – bvitg e.V. (bvitg) hat die Kanzlei Piltz Rechtsanwälte PartGmbB (Piltz Legal) Anfang 2024 mit der Erstellung eines Gutachtens[1] beauftragt. In dem Gutachten hat Piltz Legal Fragen der Mitglieder des bvitg beantwortet. Die beantworteten Fragen adressieren verschiedene Vorgaben aus § 393 SGB V. Im Ihnen vorliegenden FAQ-Dokument wurden wesentliche Erkenntnisse aus dem Gutachten aufbereitet. Bei Rückfragen können Sie sich gerne an Philipp Quiel (philipp.quiel@piltz.legal) als Ansprechpartner bei Piltz Legal oder auch an Tom Lühmann als Ansprechpartner beim bvitg (tom.luehmann@bvitg.de) wenden.

FAQ zum Gutachten in Bezug auf Vorgaben aus § 393 SGB V

Muss ich mich mit den Vorgaben aus § 393 SGB V auseinandersetzen, wenn ich keinen Cloud-Computing-Dienst für die Verarbeitung von Sozial- und Gesundheitsdaten nutze? Und was ist, wenn ich einen Cloud-Computing-Dienst nutze, aber keine Sozial- und keine Gesundheitsdaten mit dem Dienst verarbeite?

Nein, der § 393 SGB V ist von vornherein nur relevant, wenn mit Cloud-Computing-Diensten Sozial- und Gesundheitsdaten verarbeitet werden. In allen anderen Fällen ist § 363 SGB V nicht anzuwenden. Wenn man beispielsweise einen Cloud-Computing-Dienst einsetzt, aber damit keine Sozial- und / oder Gesundheitsdaten verarbeitet, dann ist § 393 SGB V für diesen Anwendungsfall auch nicht relevant.

Wann gilt eine Anwendung oder Software o.ä. als ein „Cloud-Computing-Dienst"?

Wenn der Dienst ein **digitaler Dienst** ist (und nicht auf anderem Weg – etwa als klassisches physisches Housing – erbracht wird), der durch **Abruf die Verwaltung** und einen **umfassenden Fernzugang** zu einem **skalierbaren** und **elastischen** Pool **gemeinsam nutzbarer Rechenressourcen** ermöglicht.

Was ist, wenn der relevante digitale Dienst bspw. zwar einen Fernzugang zu gemeinsam nutzbaren Rechenressourcen ermöglicht, aber der Ressourcen-Pool entweder nicht skalierbar oder nicht elastisch ist?

Dann ist dieser Dienst kein Cloud-Computing-Dienst und § 393 SGB V ist für diesen Fall nicht von Bedeutung. Es müssen immer alle in der vorstehenden Antwort fett hervorgehobenen Begriffsmerkmale erfüllt sein. Schon wenn eines der vielen Merkmale nicht erfüllt ist, dann ist der relevante Dienst kein Cloud-Computing-Dienst.

Wer ist die datenverarbeitende Stelle, die gemäß § 393 Abs. 2 SGB V eine Niederlassung im Inland und gemäß Abs. 3 Nr. 2 derselben Vorschrift ein BSI-C5-Testat haben muss?

Der Gesetzgeber hat es unnötig kompliziert gemacht: Der Begriff „datenverarbeitende Stelle " ist nicht definiert und die Bedeutung des Begriffs wird vom Gesetzgeber in den Gesetzesmaterialien nirgendwo erläutert. Wie im Gutachten ausgeführt wurde, sprechen die deutlich besseren Argumente dafür, dass der Verantwortliche i.S.v. Art. 4 Nr. 7 DSGVO die „datenverarbeitende Stelle" i.S.d. § 393 SGB V ist. Das sind in fast allen Fällen die Unternehmen, öffentlichen Stellen, Verbände und andere Institutionen, die einen von einem Dritten angebotenen Cloud-Computing-Dienst nutzen. Anbieter und Hersteller dieser Dienste sind nach diesem Verständnis keine datenverarbeitenden Stellen i.S.v. § 393 SGB V.

[1]Gutachten zu Fragen der Mitglieder des Bundesverband Gesundheits-IT – bvitg e.V.
Stand: 2. Mai 2024. Online verfügbar, abrufbar unter https://www.bvitg.de/wp-content/uploads/2024-05-27_bvitg-Cloud-Gutachten.pdf

Wofür wird ein BSI-C5-Testat ausgestellt: Für einen Dienst oder für eine datenverarbeitende Stelle oder für den Einsatz eines Dienstes bei einer datenverarbeitenden Stelle?

Die datenverarbeitende Stelle muss zwar das Vorliegen eines BSI-C5-Testats nachweisen. Die Testierung an sich erfolgt jedoch für die im Rahmen des Cloud-Computing-Dienstes eingesetzten Cloud-Systeme und die eingesetzte Technik. Daher muss zwar die datenverarbeitende Stelle das Vorliegen eines BSI-C5-Testats nachweisen, aber testiert werden nicht datenverarbeitende Stellen als solche, sondern die Cloud-Systeme und eingesetzte Technik.

Ist es möglich, mit Cloud-Computing-Diensten Sozial- oder Gesundheitsdaten zu verarbeiten, ohne dass der Dienst nach BSI-C5 testiert ist?

Ja, Piltz Legal ist – entgegen anderslautenden Ansichten – fest davon überzeugt, dass der § 393 SGB V nur eine von mehreren möglichen Rechtsgrundlagen ist. Wenn man sich für die Verarbeitung von Sozial- oder Gesundheitsdaten vor Einführung des § 393 SGB V auf eine andere Rechtsgrundlage berufen konnte, dann bleibt das auch nach Einführung der Vorschrift möglich.

Wenn es kein BSI-C5-Testat gibt: Welche Sicherheitsmaßnahmen werden benötigt?

Nur weil man kein BSI-C5-Testat benötigt, bedeutet dies nicht, dass die zu implementierenden Sicherheitsmaßnahmen weniger stark sein können. Das Gegenteil ist der Fall. Art. 32 DSGVO und andere Bestimmungen aus dem SGB V verpflichten genauso zur Gewährleistung eines angemessenen Schutzniveaus. Ein Testat eines Wirtschaftsprüfers wird dann aber nicht benötigt.

Was ist bei Datenübermittlungen in Länder außerhalb der EU und des EWR zu beachten?

Wenn Datenübermittlungen in Länder außerhalb der EU und des EWR vorgenommen werden, muss für das relevante Land oder eine konkrete Partei im Drittland (wie etwa beim Data Privacy Framework) ein Angemessenheitsbeschluss gelten. Bei Anwendung von § 393 SGB V ist es u.a. nicht möglich, Standardvertragsklauseln oder Binding Corporate Rules zu verwenden.

Wenn ich Rückfragen zu dem Thema habe, an wen kann ich mich dann wenden?

Philipp Quiel (philipp.quiel@piltz.legal) oder Tom Lühmann (tom.luehmann@bvitg.de).

Über den Bundesverband Gesundheits-IT - bvitg e. V.

Der bvitg vertritt in Deutschland die führenden Anbieter von Gesundheits-IT und ist Veranstalter der DMEA, Europas wichtigster Veranstaltung für Health-IT. Mit rund 110 Mitgliedern arbeiten wir gemeinsam daran, die Gesundheits-IT für alle Versorgungsbereiche zu etablieren, um so die Gesundheitsversorgung der Menschen in Deutschland nachhaltig zu verbessern.

Tom Lühmann
tom.luehmann@bvitg.de

www.bvitg.de

Über die Kanzlei Piltz Legal

Piltz Legal ist eine mittelständische u.a. auf die Bereiche Datenschutzrecht, IT-Recht und Gesundheitsdatenschutz spezialisierte Kanzlei aus Berlin. Wir unterstützen unsere Mandanten mit Leidenschaft für unsere Fachgebiete, Neugier auf neue Herausforderungen und Engagement für die Interessen unserer Mandanten. Unser Ziel ist es immer, mit lösungsorientiertem Pragmatismus nachhaltige Ergebnisse für unsere Mandanten zu erreichen.

Philipp Quiel
philipp.quiel@piltz.legal

www.piltz.legal