Digitalisierung – juristische Aspekte

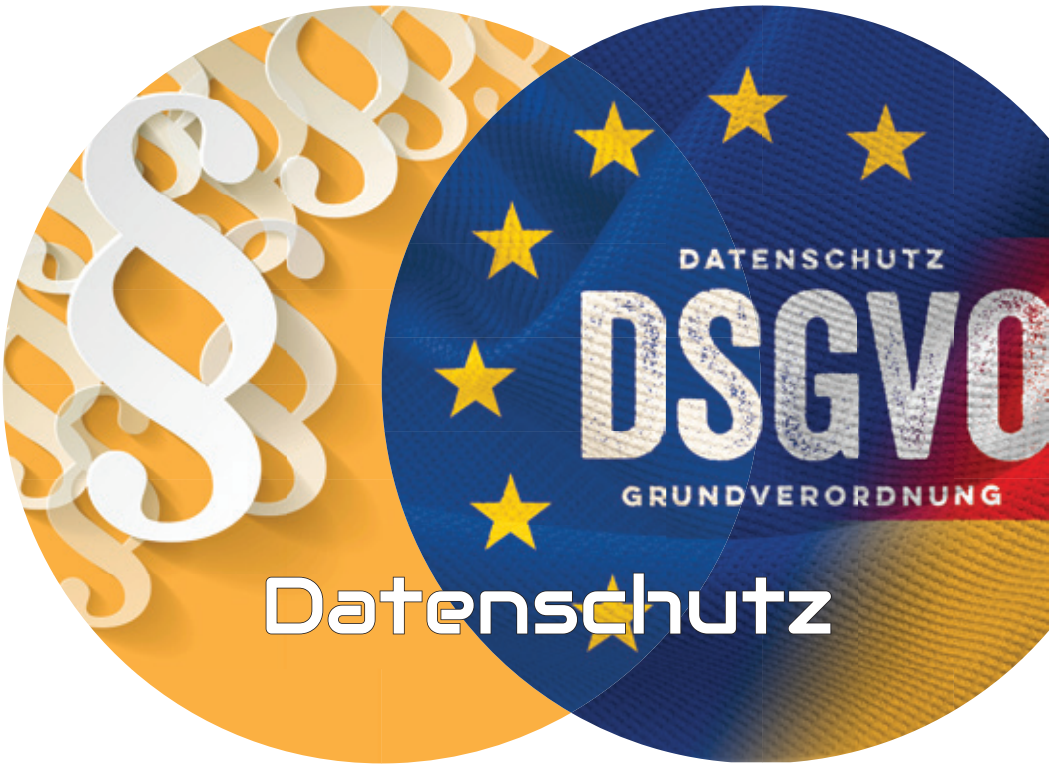
Die Digitalisierung wirft zwangsläufig datenschutzrechtliche Fragen auf – dies gilt vor allem in der Diabetologie wegen des Umfangs und der Sensibilität der dort verarbeiteten Patientendaten. Das Inkrafttreten der Datenschutzgrundverordnung der EU (DSGVO) [EU 2016] am 25. Mai 2018 hat zu einer besonderen Sensibilisierung der Öffentlichkeit für datenschutzrechtliche Fragen geführt, aber auch eine große Verunsicherung ausgelöst.

Dr. Thorsten Thaysen, München

Diabetes ist eine Datenmanagement-Krankheit. Diabetologen gehen nicht nur mit großen Mengen von Patientendaten um, sondern diese Daten ermöglichen einen tiefen Blick in die private Lebensgestaltung der Patienten und sind deswegen besonders sensibel.

Diabetes-Daten: tiefer Blick ins private Leben

Früher mögen diese Datensammlungen eventuell ein „Datenfriedhof" gewesen sein. Die digitale Datenverarbeitung ermöglicht es in einem bisher nicht bekannten Maß, Daten in kürzester Zeit auszuwerten, Profile zu erkennen und Rückschlüsse auf Verhaltensweisen von Patienten zu ziehen. Hinzu kommt eine erhebliche Verbesserung der Datenqualität und Überwachungsdichte. Es werden also nicht nur mehr, sondern auch bessere Daten gesammelt. Die aus digitalen Quellen gewonnenen Erkenntnisse können schon zu einer Verbesserung der Versorgung und Behandlung von Patienten führen [Dänschel 2018]. Digitale Prozesse halten auch in den administrativen Praxisalltag Einzug – von



der Terminvereinbarung über das Management der Patientenakten bis hin zur Kommunikation mit Patienten und Kollegen. Die Digitalisierung in der Diabetologie bringt damit erhebliche Vorteile und Chancen mit sich, erfordert aber auch eine intensivere Betrachtung rechtlicher Rahmenbedingungen.

Entwicklung des Datenschutzrechts

Die Digitalisierung berührt verschiedene Rechtsgebiete, in besonderer Weise jedoch das Datenschutzrecht. Bereits im Jahr 1983 stellte das Bundesverfassungsgericht in seinem berühmten Urteil zur Volkszählung 1983 fest, dass „es unter den Bedingungen der automatischen Datenverarbeitung kein ‚belangloses' Datum mehr [gibt]" [Bundesverfassungsgericht 1983]. In der Folgezeit stieg die Bedeutung des Datenschutzrechts sowohl in der öffentlichen Diskussion also auch in der Wahrnehmung der Gesetzgeber immer weiter. Es entstanden in Deutschland Datenschutzgesetze auf Landesebene sowie ein Bundesdatenschutzgesetz. Im Jahr 1995 erließ die damalige Europäische Gemeinschaft eine Datenschutzrichtlinie, die zu einer Vereinheitlichung der datenschutzrechtlichen Bestimmungen in den Mitgliedsstaaten beitragen sollte, insbesondere sollte durch ein einheitliches (Mindest-)Schutzniveau für personenbezogene Daten der freie Fluss personenbezogener Daten innerhalb der Europäischen Union sichergestellt werden. Richtlinien der Europäischen Union gelten nicht unmittelbar gegenüber den Betroffenen (also den Bürgern), sondern müssen erst durch die Mitgliedsstaaten in ihre jeweilige Rechtsordnung umgesetzt werden.

Die Digitalisierung berührt verschiedene Rechtsgebiete, in besonderer Weise jedoch das Datenschutzrecht.

Die Folge daraus war, dass in der Europäischen Union viele unterschiedliche Regelungen zum Datenschutz bestanden. Als Konsequenz daraus entschied die Europäische Union, das Datenschutzrecht durch eine Verordnung zu regeln.

Eine Verordnung gilt anders als eine Richtlinie unmittelbar gegenüber den Betroffenen und bedarf grundsätzlich keiner Umsetzung durch die Mitgliedsstaaten. Die DSGVO gilt somit als Verordnung direkt und unmittelbar in der gesamten Europäischen Union. Jedoch enthält sie ca. 80 Öffnungsklauseln, also Vorschriften, die den Mitgliedsstaaten eigene Regelungen erlauben. Daher ist es erforderlich, z. B. in Deutschland neben der DSGVO auch noch das Bundesdatenschutzgesetz (BDSG) und ggf. auch die Landesdatenschutzgesetze zu prüfen, wenn es um das Beantworten einer datenschutzrechtlichen Frage geht.

Aktuelle Herausforderungen

Der Fortschritt der Digitalisierung und der damit verbundene Zuwachs an technischen Möglichkeiten waren seit dem Jahr 1983 enorm. Die Gesetzgeber auf europäischer und nationaler Ebene bemühen sich zwar, mit dieser Entwicklung Schritt zu halten und die Datenschutzgesetze „technikneutral" zu formulieren, letztlich ist die technische Entwicklung aber immer weiter als die rechtliche Gestaltung in den Datenschutzgesetzen.

Die Digitalisierung ermöglicht eine Sammlung und Auswertung personenbezogener Daten in vorher nicht gekanntem Ausmaß.

Unabhängig davon ergeben sich auch Zielkonflikte zwischen den Möglichkeiten der Digitalisierung und den Grundprinzipien des Datenschutzes. Während die Digitalisierung eine Sammlung und Auswertung personenbezogener Daten in vorher nicht gekanntem Ausmaß ermöglicht, verlangt das Datenschutzrecht ei-

ne Limitierung des Umfangs der Datenerhebung auf das absolut Notwendige (Datensparsamkeit) und eine Limitierung der Datennutzung auf konkrete, vorher festgelegte Zwecke (Zweckbindung). Die Digitalisierung erleichtert generell die Verarbeitung personenbezogener Daten, während das Datenschutzrecht verlangt, dass eine gesetzliche Bestimmung (z. B. in Datenschutzgesetzen) das Verarbeiten von personenbezogenen Daten erlaubt. Vor dem Hintergrund eines erheblich gestiegenen Bußgeldrahmens (von bisher maximal 300 000 € unter dem alten BDSG auf nunmehr maximal 20 000 000 €, Art. 83 DSGVO) ist der Ausgleich dieser Konfliktlagen eine der größten Herausforderungen der Digitalisierung – gerade in der Diabetologie.

Personenbezogene Daten

Datenschutzrechtliche Vorgaben gelten nur für „personenbezogene Daten". Dabei handelt es sich um den zentralen Begriff des Datenschutzrechts. „Personenbezogene Daten" sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 Nr. 1 DSGVO). Diese Person wird im Datenschutzrecht „Betroffener" genannt. Informationen beziehen sich auf eine identifizierte natürliche Person, wenn sie diese Person unmittelbar identifizieren (z. B. der Name).

„Personenbezogene Daten" sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

Demgegenüber beziehen sich Informationen auf eine identifizierbare natürliche Person, wenn die Information die Person mittelbar, also durch Hinzunahme weiterer Informationen, identifiziert (z. B. ist die Telefonnummer regelmäßig nur mittelbar zur Identifizierung von Personen geeignet, weil es dafür der Zusatzinformation bedarf, wer Inhaber des Anschlusses ist). Wenn eine Information weder unmittelbar noch mittelbar eine natürliche Person identifiziert, unterliegt diese Information keinen datenschutzrechtlichen Bindungen, d. h. diese Information kann verarbeitet werden, ohne dass das Datenschutzrecht beachtet werden muss. Dies ist zum Beispiel immer dann der Fall, wenn Informationen über mehrere Personen zusammengefasst (aggregiert) werden, etwa im Rahmen von Statistiken (z. B. Anzahl der Patienten mit einem bestimmten HbA_{1c}-Wert in einer Praxis). Allerdings setzt dies voraus, dass die Anzahl der Personen, deren Daten aggregiert werden, so groß ist, dass ein Rückschluss auf die einzelne Person nicht mehr möglich ist. Wenn z. B. in der HbA_{1c}-Statistik nur zwei Patienten einen bestimmten HbA_{1c}-Wert haben, ist eine mittelbare Identifizierbarkeit regelmäßig gegeben, so dass weiterhin datenschutzrechtliche Vorgaben zu beachten sind. Bei der Prüfung, ob es sich um „personenbezogene Daten" handelt, ist besondere Vorsicht anzuraten. Denn ein irrtümlicher Ausschluss des Personenbezugs von Daten führt regelmäßig zur Nichteinhaltung datenschutzrechtlicher Vorgaben und damit zu einer rechtswidrigen Datenverarbeitung. Daher sollte im Zweifel immer von einem Personenbezug von Daten ausgegangen werden.

Verarbeitung personenbezogener Daten

Das Datenschutzrecht knüpft weiter an den Begriff der „Verarbeitung" personenbezogener Daten an. In der Praxis ist immer wieder zu beobachten, dass der Begriff der „Verarbeitung" zu eng interpretiert wird. Eine „Verarbeitung" im datenschutzrechtlichen Sinn umfasst jedoch

jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten (Art. 4 Nr. 2 DSGVO). Darunter fällt z. B. das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung. Es handelt sich also um einen weitgefassten Begriff, der jeden Umgang mit personenbezogenen Daten umfasst. Derjenige, der über die Zwecke und Mittel der Verarbeitung bestimmt, ist der „Verantwortliche" und damit verpflichtet, die datenschutzrechtlichen Vorgaben umzusetzen und einzuhalten (Art. 4 Nr. 7 DSGVO).

Erlaubnistatbestände

Jede Verarbeitung personenbezogener Daten ist nur zulässig, wenn eine gesetzliche Bestimmung dies erlaubt. Die DSGVO sieht dazu verschiedene Erlaubnistatbestände vor (z. B. Art. 6 DSGVO), allerdings können sich Erlaubnistatbestände auch aus anderen Gesetzen ergeben (z. B. bei gesetzlich Versicherten aus dem SGB V). In der diabetologischen Praxis relevante Erlaubnistatbestände aus der DSGVO sind z. B. die Einwilligung des Betroffenen (Art. 6 Abs. 1 S. 1 lit. a DSGVO), die Erfüllung eines Vertrags mit dem Betroffenen (z. B. des ärztlichen Behandlungsvertrags) (Art. 6 Abs. 1 S. 1 lit. b DSGVO), der Schutz lebenswichtiger Interessen des Betroffenen (z. B. bei medizinischen Notfällen) (Art. 6 Abs. 1 S. 1 lit. d DSGVO) oder zur Wahrung berechtigter Interessen, sofern nicht die Interessen des Betroffenen an dem Schutz seiner Daten überwiegen (Art. 6 Abs. 1 S. 1 lit. f DSGVO). Diese Regelungen galten im Wesentlichen auch schon vor Inkrafttreten der DSGVO. Neu ist jedoch die „Rechenschaftspflicht": Jeder Verantwortliche muss nachweisen können, dass er die Anforderungen der DSGVO einhält (Art. 5 Abs. 2 DSGVO), also insbesondere die von ihm vorgenommenen Datenverarbeitungen auf einen Erlaubnistatbestand stützen kann.

Einwilligung des Betroffenen

Die Einwilligung des Betroffenen wird in der Praxis oft als wichtigster Erlaubnistatbestand angesehen. Dabei wird allerdings übersehen, dass das Einholen einer Einwilligung nicht er-

forderlich ist, wenn die jeweilige Datenverarbeitung bereits auf einen anderen Erlaubnistatbestand gestützt werden kann. Wenn ein anderer Erlaubnistatbestand eingreift, sollte das Einholen einer Einwilligung unterlassen werden. Datenschutzrechtliche Einwilligungen sind grundsätzlich jederzeit frei widerruflich. Wenn der Betroffene von seinem Widerrufsrecht Gebrauch macht, muss die jeweilige Datenverarbeitung beendet werden. Denn die Verarbeitung darf dann nicht mehr auf einen anderen Erlaubnistatbestand gestützt werden, weil sonst der Betroffene nicht frei über die Verarbeitung seiner Daten entscheiden könnte. Gerade diese freie Entscheidung über die Datenverarbeitung ist aber Kernmerkmal der Einwilligung. Räumt der Verantwortliche dem Betroffenen also durch das Abfragen der Einwilligung das Recht ein, über die Verarbeitung seiner Daten selbst zu entscheiden, muss der Verantwortliche auch akzeptieren, dass der Betroffene sich dafür entscheidet, die Datenverarbeitung zu beenden.

Der Betroffene muss abschätzen können, welche Daten betroffen sind, wie umfangreich die jeweilige Datenverarbeitung ist und zu welchen Zwecken diese erfolgt.

Eine datenschutzrechtliche Einwilligung muss bestimmte Bedingungen erfüllen, um wirksam zu sein. Dazu gehört, dass der Betroffene umfassend über die jeweilige Datenverarbeitung informiert sein muss („Informiertheit der Einwilligung"), d. h. der Betroffene muss abschätzen können, welche Daten betroffen sind, wie umfangreich die jeweilige Datenverarbeitung ist und zu welchen Zwecken diese erfolgt. Des Weiteren muss die Einwilligung freiwillig erteilt werden („Freiwilligkeit"), d. h. der Betroffene darf nicht unter Zwang stehen, muss also tatsächlich frei entscheiden können, ob er die Einwilligung erteilt. Schließlich muss die Einwilligung auch eindeutig erklärt werden („Eindeutigkeit"), d. h. es muss dem Betroffenen bewusst sein, dass er mit einer bestimmten Handlung eine Einwilligung in eine Datenverarbeitung erteilt.

Die Einwilligung ist an keine bestimmte Form gebunden, muss also nicht zwingend schriftlich eingeholt werden. Allerdings gilt auch hier die bereits oben genannte Rechenschaftspflicht, d. h. wenn der Verantwortliche eine Datenverarbeitung auf eine Einwilligung des Betroffenen stützen will, muss der Verantwortliche nachweisen können, dass der Betroffene ihm eine Einwilligung erteilt hat (Art. 7 Abs. 1 DSGVO).

In der diabetologischen Praxis ist das Einholen datenschutzrechtlicher Einwilligungen vor allem zur Kommunikation mit Patienten und bei Privatpatienten zur Abrechnung erbrachter Leistungen notwendig.

In der diabetologischen Praxis ist das Einholen datenschutzrechtlicher Einwilligungen vor allem zur Kommunikation mit Patienten über unverschlüsselte E-Mails und bei Privatpatienten zur Abrechnung der erbrachten Leistungen über einen Abrechnungsdienstleister notwendig. Hinzu kommt bei gesetzlich Versicherten das Erfordernis einer Einwilligung zum Datenaustausch zwischen Hausarzt und anderen Leistungserbringern (§73 Abs. 1b SGB V).

Erfüllung eines Vertrags mit dem Betroffenen

Auf diesen Erlaubnistatbestand können die meisten Verarbeitungen gestützt werden, die keine medizinischen Daten von Patienten (besondere Kategorien personenbezogener Daten) enthalten. Entscheidend ist, dass die jeweiligen Daten für das Durchführen des Behandlungsvertrags benötigt werden. Dies betrifft zum Beispiel das Erfassen der Stammdaten von Patienten oder die reine Terminverwaltung (soweit dabei keine Diagnosen oder Beschwerden erfasst werden).

Wahrung berechtigter Interessen

Dieser Erlaubnistatbestand ermöglicht die Verarbeitung von Patientendaten, die zwar nicht unmittelbar dem Durchführen des Behandlungsvertrags dienen, an deren Verarbeitung aber ein berechtigtes Interesse des Diabetologen besteht. Darunter fällt zum Beispiel das namentliche Aufrufen von Patienten im Wartezimmer. Medizinische Daten von Patienten (besondere Kategorien personenbezogener Daten) dürfen jedoch nicht auf Grundlage dieses Erlaubnistatbestands verarbeitet werden.

Besondere Kategorien personenbezogener Daten

Grundsätzlich unterscheidet das Datenschutzrecht nicht zwischen verschiedenen Arten personenbezogener Daten. Die möglicherweise unterschiedliche Relevanz bestimmter personenbezogener Daten für die jeweils Betroffenen wird grundsätzlich erst im Rahmen der Prüfung bestimmter datenschutzrechtlicher Erlaubnisnormen berücksichtigt, etwa bei der Interessenabwägung im Rahmen des Erlaubnistatbestands der Wahrung berechtigter Interessen. Es gibt jedoch eine Ausnahme: Bestimmte personenbezogene Daten sind aus Sicht des Datenschutzrechts als besonders sensibel anzusehen und werden daher als „besondere Kategorien personenbezogener Daten" von vornherein einem besonders strengen Schutz unterstellt (Art. 9 DSGVO). Es handelt sich dabei um personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie um genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

In der diabetologischen Praxis kommen besondere Kategorien personenbezogener Daten besonders häufig in Form von Gesundheitsdaten und genetischen Daten vor.

In der diabetologischen Praxis kommen daher besondere Kategorien personenbezogener Daten besonders häufig in Form von Gesundheitsdaten und genetischen Daten vor. Das Datenschutzrecht gestattet eine Verarbeitung besonderer Kategorien personenbezogener Daten nur in wenigen, eng definierten Ausnahmefällen. Dazu gehören z. B. die medizinische Diagnostik und die Versorgung oder Behandlung im Gesundheitsbereich, soweit eine Verarbeitung besonderer Kategorien personenbezogener Daten dafür erforderlich ist und die jeweiligen Maßnahmen durch einen Arzt oder unter der Verantwortung eines Arztes durchgeführt werden (Art. 9 Abs. 2 S. 1 lit. h, Abs. 3 DSGVO). Insofern ist in der diabetologischen Praxis meistens eine datenschutzrechtliche Rechtfertigung zum Umgang mit den Patientendaten gegeben.

Datensicherheit

Neben den Vorgaben zur Zulässigkeit der Datenverarbeitung an sich, also das „Ob" der Datenverarbeitung, bestimmen die Vorgaben zur Datensicherheit die Art des Umgangs mit den Daten während der Verarbeitung, also das „Wie" der Datenverarbeitung. Der Verantwortliche ist verpflichtet, geeignete und angemessene technische und organisatorische Maßnahmen zu treffen, um die Sicherheit der von ihm verarbeiteten personenbezogenen Daten sicherzustellen (Art. 32 DSGVO). Die Maßnahmen müssen an dem Schutzbedarf der jeweiligen Daten ausgerichtet werden. Beispiele für solche Maßnahmen sind Zugriffs- und Berechtigungskonzepte für IT-Systeme (z. B. Absicherung der Computersysteme in der Praxis durch aktuelle Sicherheitssoftware und Passwörter, Zugriffsbeschränkungen innerhalb von IT-Systemen) und Zugriffssicherungen für physische Datenquellen (z. B. verschlossene Ablage für Patientenakten, Ablage der Akten direkt nach der Benutzung). Dazu gehören auch Vorgaben für den Versand von Patientendaten (z. B. kein Versand per unverschlüsselter E-Mail ohne informierte Einwilligung des Patienten).

Zusammenfassung und weiterführende Links

Verglichen mit der bisherigen Rechtslage in Deutschland hat die DSGVO die datenschutzrechtlichen Anforderungen nicht wesentlich verschärft, jedoch durch die Einführung der Rechenschaftspflicht und des erheblich höheren Bußgeldrahmens den Umsetzungsdruck stark erhöht. Dadurch hat das Thema Datenschutz seit Inkrafttreten der DSGVO insgesamt eine deutlich höhere Beachtung erfahren. Erste Gerichtsentscheidungen stehen allerdings noch aus, und auch behördliche Verlautbarungen zu konkreten Anwendungsfragen sind eher noch selten. Hier bleibt abzuwarten, welche Entwicklung das Datenschutzrecht nehmen wird und wie sich dies auf die Digitalisierung auswirken wird.

Weiterführende Informationen

sind unter folgenden Links verfügbar:

- Kassenärztliche Bundesvereinigung: http://www.kbv.de/html/datensicherheit.php
- Bundesärztekammer: http://www.bundesaerztekammer.de/recht/aktuelle-rechtliche-themen/datenschutzrecht/
- Deutsche Diabetes Gesellschaft: https://www.deutsche-diabetes-gesellschaft.de/gesundheitspolitik/code-of-conduct-digital-health-der-ddg.html
- Bayerisches Landesamt für Datenschutzaufsicht:
  https://www.lda.bayern.de/media/DS-GVO_in_Arztpraxen.pdf
  https://www.lda.bayern.de/media/muster_5_arztpraxis.pdf
  https://www.lda.bayern.de/media/muster_5_arztpraxis_verzeichnis.pdf

Quellen

1. *EU: Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016. https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=EN (Zugriff: 18.12.2018)*
2. *Dänschel I, Dänschel W, Heinemann L, Weissmann J, Kulzer B: Effects of Integrated Personalized Diabetes Management: Results of the PDM-Pro-Value study program. 15th International Primary Care Diabetes Europe Conference, 13–14 April 2018, Barcelona, Spain: Poster 1261*
3. *Bundesverfassungsgericht: BVerfGE 65, 1 – Volkszählung. Urteil vom 15.12.1983, 1 BvR 209/83, BVerfGE 65, 1 (45). http://www.servat.unibe.ch/dfr/bv065001.html (Zugriff: 18.12.2018)*