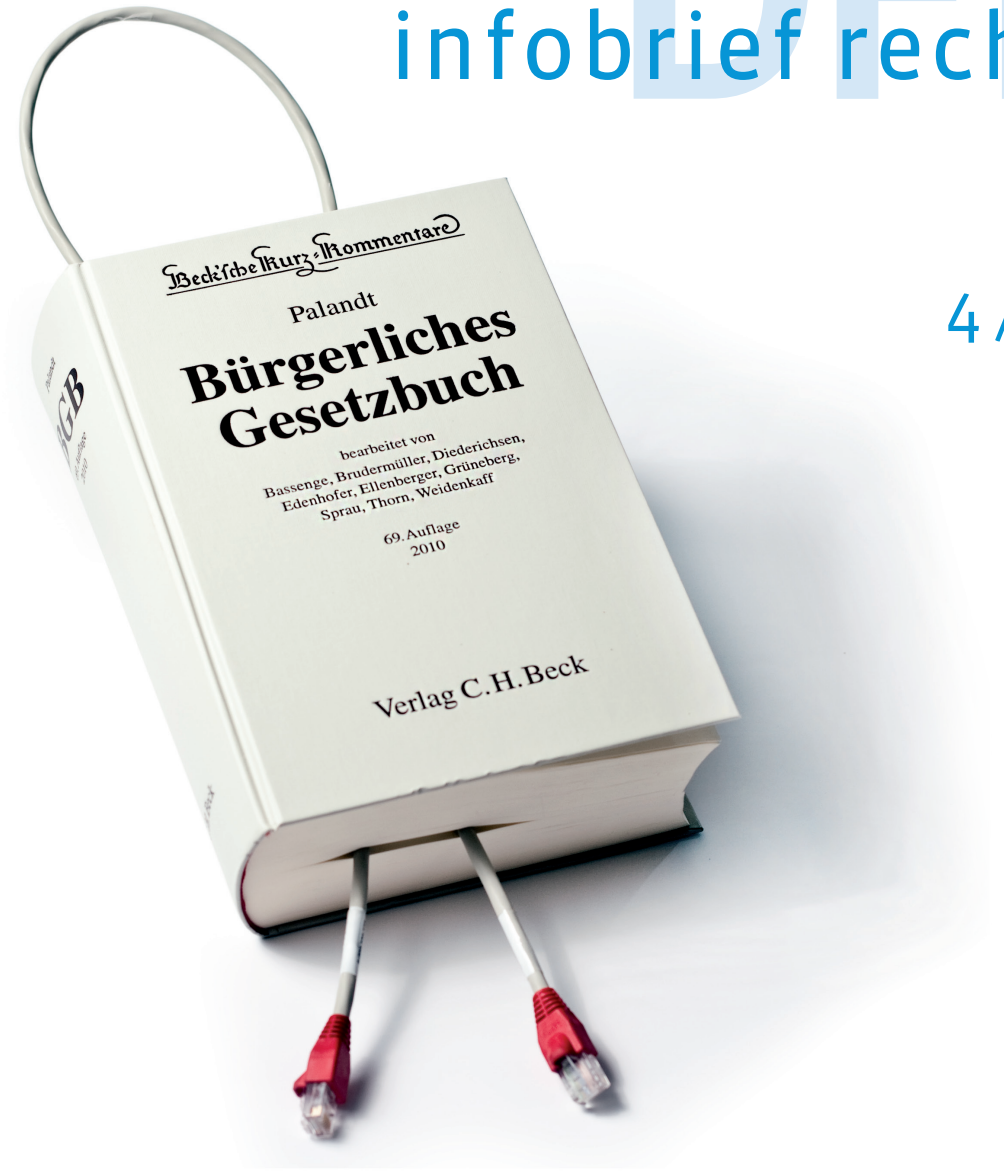
infobrief recht

4 / 2018
April 2018



Auf die Methode kommt es (nicht) an!

OLG Frankfurt a. M. urteilt zur vertragsrechtlichen Einordnung von Programmierleistungen nach der Scrum-Methode

Zuhause ist es am Schönsten, auch für personenbezogene Daten!

Zum datenschutzrechtskonformen Einsatz des Webanalysetools Matomo (PIWIK) nach der DSGVO

Her damit!

Europäischer Gerichtshof qualifiziert Antworten eines Prüflings in einer berufsbezogenen Prüfung und die dazugehörigen Anmerkungen des Prüfers als personenbezogene Daten

Auf die Methode kommt es (nicht) an!

OLG Frankfurt a. M. urteilt zur vertragsrechtlichen Einordnung von Programmierleistungen nach der Scrum-Methode

von Matthias Mörike

Softwareprojekte werden zunehmend mithilfe sogenannter agiler Methoden realisiert, um möglichst flexibel auf Änderungswünsche eingehen und möglichst kurze Arbeitsschritte durchführen zu können. Auch solche Vorgehensweisen benötigen einen vertragsrechtlichen Rahmen. Die bisherige Einordnung von Softwareerstellungsverträgen als Werkverträge ist nicht selbstverständlich, gewinnt aber durch ein kürzlich ergangenes Urteil des OLG Frankfurt a. M. wieder an Bedeutung. Es ist wahrscheinlich, dass die weitere Entwicklung, insbesondere ein abschließendes Urteil des BGH, zu mehr Klarheit führen wird.

I. Wasserfall-Modell und Scrum-Methode

Softwareentwicklung ist naturgemäß eng mit dem technischen Fortschritt verbunden. Die dadurch verursachten Veränderungen wirken sich nicht nur auf die technischen Programmiermöglichkeiten selbst, sondern auch auf die Programmiermethodik aus. Traditionell wurde und wird Software nach dem Wasserfall-Modell entwickelt. Dieses Modell umfasst üblicherweise folgende Entwicklungsphasen: Anforderungsanalyse, Systemdesign, Programmierung, Programmtest und Programmeinsatz. Der Vorteil dieses Modells ist, dass der Auftraggeber präzise Vorgaben bezüglich des Funktionsumfangs der gewünschten Software erstellt. Liegen solche Vorgaben vor, kann der Erfolg einer Programmierleistung einfach daran gemessen werden, ob das erstelle Produkt die Vorgaben erfüllt. Dieser Vorteil ist zugleich der große Nachteil des Modells. Häufig weiß ein Auftraggeber zwar, wofür er die Software einsetzen will. Welche Funktionen genau in Frage kommen und welche davon für ihn am sinnvollsten sind, kann er mangels entsprechender Fachkenntnis jedoch häufig nicht selbst bestimmen. Hinzu kommt, dass es während eines langfristigen Softwareprojekts häufig zu Änderungswünschen kommt. Im schlimmsten Fall muss der gesamte Programmierprozess neu begonnen werden. Diesen Nachteilen des Wasserfall-Modells begegnen sogenannte agile Programmiermethoden. Ein bekanntes Beispiel dafür ist das Scrum-Verfahren. Dabei arbeiten die Vertragsparteien nicht mit starren Vorgaben, sondern entwickeln die Anforderungen im Laufe des Projekts gemeinsam. Auch wird nicht am Ende ein umfassendes Softwareprodukt abgeliefert, sondern vielmehr in möglichst kurzen Abständen einzelne, für sich selbst funktionsfähige Softwareteile, die dann sukzessive zusammengefügt werden, erstellt. Dadurch können Änderungswünsche leichter berücksichtigt werden. Außerdem werden die negativen Folgen einer vorzeitigen Beendigung des Projekts begrenzt. Es besteht keine Gefahr, dass alle bisherigen Arbeiten wertlos werden, da die bereits abgeschlossenen Komponenten genutzt und gegebenenfalls weiterentwickelt werden können.

II. Rechtliche Problemstellung

Wird Software nach den individuellen Wünschen des Bestellers angefertigt, handelt es sich beim zugrunde liegenden Vertrag in der Regel um einen Werkvertrag gemäß §§ 631 ff. Bürgerliches Gesetzbuch (BGB). Der Besteller bestimmt in einem Pflichten- und Lastenheft, welche Funktionen die Software erfüllen soll, zudem sollte der Vertrag die Vergütung und den Übergang von Nutzungsrechten regeln (siehe dazu Mörike, Wer erntet die Früchte? – Teil 2, DFN Infobrief Recht 01/2018). Der Auftragnehmer schuldet im Gegenzug die Erstellung der Software mit allen vereinbarten Funktionen.

Wichtig bei Werkverträgen ist die Abnahme des erstellten Werkes durch den Besteller (§ 640 BGB). Erst dann kann der Auftragnehmer grundsätzlich die Vergütung verlangen. Eine Abnahme liegt im Wesentlichen dann vor, wenn der Besteller das Werk als vertragsgemäß akzeptiert. Dies kann, muss aber nicht ausdrücklich erfolgen. Eine anderweitige bestätigende Handlung genügt unter Umständen ebenso.

Softwareverträge bezüglich agiler Programmiermethoden lassen sich nicht ohne weiteres als Werkvertrag einordnen. Es fehlt insoweit an den für einen Werkvertrag eigentlich typischen Vorgaben des Bestellers. In der Literatur werden das Dienstvertragsrecht (§§ 611 ff. BGB) und das Gesellschaftsrecht (§§ 705 ff. BGB) diskutiert. Das Oberlandesgericht (OLG) Frankfurt a. M. hatte über einen Fall zu urteilen, der genau diese Problematik zum Gegenstand hatte. Überraschenderweise tendiert das Gericht auch in den Verträgen über Programmleistungen nach dem Scrum-Verfahren zu einer werkvertraglichen Einordnung.

III. Sachverhalt der Entscheidung

Die Beklagte beabsichtigte, eine Internetplattform zu erstellen. Die Klägerin führte zwischen September 2012 und Januar 2013 dafür Programmierleistungen durch. Die Parteien beendeten die Zusammenarbeit vor Fertigstellung des Projekts, waren sich jedoch einig darüber, dass die bis dahin vereinbarten Leistungen erbracht wurden. Im „Letter of Intent" hatten die Parteien bestimmt, die Programmierarbeiten nach dem Scrum-Verfahren durchzuführen. Der eigentliche Projektvertrag wurde zwar verhandelt und ausgefertigt, jedoch nicht unterzeichnet. Im April 2013, nach Beendigung des Projekts, schlossen die Parteien eine Ratenvereinbarung über die ausstehende Vergütung. Die Beklagte hat die Raten nicht vereinbarungsgemäß beglichen, weswegen die Klägerin versucht, die ausstehenden Raten gerichtlich durchzusetzen.

IV. Entscheidung des Gerichts

Während die erste Instanz, das Landgericht (LG) Wiesbaden, der Klägerin einen Anspruch auf die ausstehenden Raten noch versagte (LG Wiesbaden, Urteil vom 30.11.2016, Az. 11 O 10/15), hat das OLG Frankfurt a. M. der Klage und damit dem Anspruch des Klägers im Rahmen der Berufung stattgegeben (OLG Frankfurt a. M., Urteil vom 17.08.2017, Az. 5 U 152/16). Beide Gerichte sahen in dem unterzeichneten „Letter of Intent" und dem tatsächlichen Durchführen der Arbeiten eine ausreichende Grundlage für einen Vertragsschluss zwischen den Parteien. Es war insofern unschädlich, dass der Projektvertrag nie unterzeichnet wurde. Während das LG Wiesbaden den Vertrag als Werkvertrag gemäß §§ 631 ff. BGB einordnete, lies das OLG Frankfurt a. M. diese Einordnung allerdings im Ergebnis offen, da sie für die im Prozess zu klärende Frage letzten Endes nicht von Bedeutung war. Nichtsdestotrotz hat auch das OLG Frankfurt a. M. eine Tendenz in Hinblick auf eine Einordnung als Werkvertrag erkennen lassen. Zwar könne der Vertrag grundsätzlich auch Dienstvertragsrecht unterfallen. Aber auch eine Einordnung als Werkvertrag sei zumindest teilweise möglich. Entscheidend für die Abgrenzung sei der Parteiwille. In dem nicht unterzeichneten Projektvertrag hätten die Parteien ausdrücklich die Geltung des Werkvertragsrechts vereinbart. Zudem könne man die Vereinbarung, nach den Vorgaben des Scrum-Verfahrens vorzugehen, dahingehend verstehen. Im vorliegenden Fall hatten die Parteien vereinbart, jeden Monat die vorzunehmenden Arbeiten zu bestimmen und am Ende des Monats einen festgelegten Betrag als Vergütung zu zahlen. Nach Auffassung des Gerichts kann die neue Beauftragung für jeden Monat gleichzeitig als Billigung der Arbeiten im letzten Monat gesehen werden. Jedenfalls könne aber die Vereinbarung der Ratenzahlung, welche die Parteien getroffen haben, als Abnahme gesehen werden. Der Anspruch auf Zahlung scheitere auch nicht daran – hier war das LG Wiesbaden noch zu einer anderen Einschätzung gekommen – dass die erstelle Software mangelhaft sei. Erstens hätte die Beklagte die entsprechenden Mängelrechte (Minderung der Vergütung, Rücktritt vom Vertrag) gelten machen müssen, was nicht geschehen ist. Zweitens sei die Software überhaupt nicht mangelhaft. Zwar fehle es an einer ausreichenden Kommentierung der Systemarchitektur, weswegen laut Sachverständigengutachten kein Dritter die Arbeiten hätte fortführen können. Das wäre jedoch nie Bestandteil der geschuldeten Leistungen gewesen. Insgesamt bejahte das OLG Frankfurt a. M. den Anspruch der Klägerin auf Zahlung der restlichen Vergütung. Inzwischen ist das Verfahren beim Bundesgerichtshof (BGH) anhängig (Az. VII ZR 203/17). Eine Entscheidung steht aber noch aus.

V. Fazit und Konsequenzen für die Praxis in wissenschaftlichen Einrichtungen

Die Entscheidung des OLG Frankfurt a. M. ist in der Literatur auf Kritik gestoßen. Gerade dem Argument, dass jede Neubeauftragung eine Billigung der bisherigen Arbeit sein soll, wurde entgegengesetzt, dass das Scrum-Verfahren auch vorsieht, vergangene Arbeiten zu ändern und zu verbessern. Das wäre nur schwer mit dem Instrument der Abnahme als Billigung der erbrachten Leistung zu vereinbaren. Allgemein gesprochen bleibt agile Programmierung ein generelles Problem im Vertragsrecht. Denn das Gericht hat keine klare Entscheidung bezüglich des Vertragstyps gefällt. Es bleibt zu hoffen, dass der BGH in dieser Hinsicht mehr Klarheit schafft. Nichtsdestotrotz enthält das Urteil auch gute Nachrichten. Die Parteien eines Softwarevertrages haben großen Spielraum bei der rechtlichen Ausgestaltung und können beispielsweise einen bestimmten Vertragstyp wählen. Ohnehin ist es empfehlenswert, einem Softwareerstellungsprojekt einen möglichst präzisen rechtlichen Rahmen zu geben. Das Urteil des OLG Frankfurt a. M. hat immerhin gezeigt, dass für Softwareprojekte, die nach der Scrum-Methode realisiert werden, verschiedene Optionen zur Verfügung stehen.

Zuhause ist es am Schönsten, auch für personenbezogene Daten!

Zum datenschutzrechtskonformen Einsatz des Webanalysetools Matomo (PIWIK) nach der DSGVO

von Johannes Baur

Viele kennen noch den Webanalysedienst PIWIK. Die Open-Source-Software erfreute sich in den letzten Jahren vor dem Hintergrund ihrer datenschutzfreundlichen Gestaltung großer Beliebtheit. Seit Januar 2018 heißt die Software Matomo und wird nach wie vor gerne eingesetzt, nicht zuletzt deshalb, weil die Analysedaten, anders als bei anderen Webanalysediensten, auf dem eigenen Server gespeichert werden. Ab dem 25. Mai 2018 unterliegt ihr Einsatz in der europäischen Union den Vorgaben der Datenschutzgrundverordnung (DSGVO). Dieser Infobrief beleuchtet den neuen Rechtsrahmen und gibt Hinweise zur datenschutzrechtskonformen Einstellung des Webanalysetools.

I. Bedeutung von Webanalysetools

Um das Verhalten ihrer Webseitenbesucher zu überwachen, setzen Webseitenbetreiber seit vielen Jahren sogenannte Webanalysetools ein. Erste Systeme entstanden bereits Mitte der 1990er Jahre. Seit 2005 steht mit Google Analytics eine Software bereit, die zunehmend umfassende Aufzeichnungen über das Nutzerverhalten der Besucher erstellen kann. Gespeichert werden können dabei u.a. die Herkunft der Nutzer anhand der IP-Adresse, die Aufrufe der Einzelseiten, die Verweildauer und die Häufigkeit der Klicks. Aus diesen Daten ziehen die Webseitenbetreiber wertvolle Informationen zur Effizienzsteigerung und Verbesserung ihres Webangebots. Auch Hochschulen und Forschungseinrichtungen greifen aus diesen Gründen zunehmend auf Webanalysetools zurück. Aus datenschutzrechtlicher Perspektive ist deren Einsatz jedoch keinesfalls unproblematisch, da eine Vielzahl personenbezogener Daten verarbeitet und dabei teilweise auch an Dritte weitergegeben wird. Bei Datenschützern standen Webanalysetools daher in der Vergangenheit häufig in der Kritik.

II. Rechtsgrundlagen für die Datenverarbeitung

Nach einer zweijährigen Übergangsphase tritt am 25. Mai 2018 in allen Mitgliedsstaaten der europäischen Union die DSGVO in Kraft. Die Normen gelten unmittelbar und verdrängen, aller Voraussicht nach, die bisherigen Datenschutzvorschriften des Telemediengesetzes (TMG). Derzeit wird auf europäischer Ebene über die Einführung einer E-Privacy-Verordnung beraten, die Schutzvorschriften für die elektronische Kommunikation regeln soll. Tritt sie in Kraft, so gehen ihre Vorschriften der DSGVO vor. Bis dahin sind Datenverarbeitungen zur Webanalyse jedoch nach der DSGVO zu beurteilen. Dies bedeutet für Webseitenbetreiber, dass Datenverarbeitungen nicht wie bisher auf die §§ 11 ff. TMG gestützt werden können, sondern nunmehr auf Art. 6 Abs. 1 DSGVO zu stützen sind[1]

Wie das TMG, sieht auch die DSGVO für Datenverarbeitungen ein grundsätzliches Verbot mit Erlaubnisvorbehalt vor. Eine Datenverarbeitung darf daher nicht stattfinden, es sei denn, es besteht eine ausdrückliche Rechtfertigungsnorm. Eine solche könnte sich für die Webanalyse zunächst in Art. 6 Abs. 1 lit. a DSGVO finden. Demnach ist die Verarbeitung

1 Zur umstrittenen Frage des Verhältnisses zwischen den datenschutzrechtlichen Vorschriften des TMG und der DSGVO, siehe bereits Baur, Heiter weiter?, in: DFN Infobrief Recht 02/2018.

personenbezogener Daten zu einem festgelegten Zweck erlaubt, soweit der Nutzer ausdrücklich eingewilligt hat. Der Einholung einer Einwilligung stehen jedoch bei Einsatz eines Webanalysetools Umsetzungsschwierigkeiten entgegen. Der Nutzer müsste bereits vor Aufruf der Webseite, beispielweise durch ein vorgeschaltetes Fenster, über den Einsatz des Tools informiert werden und seine ausdrückliche Einwilligung zur Datenverarbeitung durch ein „Opt-In“ zum Ausdruck bringen. Ein bloßes Infobanner mit einem Verweis auf die Datenschutzerklärung und die Widerspruchsmöglichkeit dagegen genügt diesen Voraussetzungen noch nicht. Eine Umsetzungsalternative mit vorheriger Einholung einer Einwilligung ist daher äußerst nutzerunfreundlich. Viele Webseitenbetreiber schrecken vor einer solchen Implementierung zurück.

Auf die Einholung einer Einwilligung kann nach der DSGVO jedoch in den Fällen des Art. 6 Abs. 1 lit. f DSGVO verzichtet werden. Nach dieser Vorschrift kann eine Verarbeitung auch dann erfolgen, wenn berechtigte Interessen des Webseitenbetreibers die Verarbeitung erforderlich machen und die Interessen, Grundrechte und Grundfreiheiten der Nutzer, die den Schutz personenbezogener Daten erfordern, nicht überwiegen. Die Vorschrift enthält jedoch keine näheren Kriterien, wie diese Interessenabwägung vorzunehmen ist. Unter der alten Rechtslage wurde § 15 Abs. 3 TMG herangezogen, der das Anlegen von Nutzerprofilen unter der Voraussetzung gestattete, dass die Daten pseudonymisiert gespeichert werden und eine Widerspruchsmöglichkeit für die Nutzer vorgesehen ist. Daten gelten nach der DSGVO dann als pseudonymisiert, wenn ein unmittelbarer Personenbezug nicht mehr besteht, jedoch durch zusätzliche Informationen herstellbar wäre. Auch die geplante E-Privacy-Verordnung enthält in ihrer Entwurfsfassung in Art. 8 eine Erlaubnis zur Datenverarbeitung zur „Messung des Webpublikums“, wenn der Betreiber der Webseite die Messung durchführt. Für die Interessenabwägung im Rahmen des Art. 6 Abs. 1 lit. f DSGVO lässt sich daher vermuten, dass das berechtigte Interesse des Webseitenbetreibers zumindest dann überwiegt, wenn er die Datenanalyse selbst durchführt, bei der Speicherung weitestgehend auf personenbezogene Daten der Nutzer verzichtet und für die Nutzer eine Widerspruchsmöglichkeit auf einfachem Wege bereithält.

Die Vorschriften der DSGVO lassen sich nach dem bisher Gesagten so interpretieren, dass unter den genannten Voraussetzungen eine Webanalyse auch auf ein berechtigtes Interesse des Webseitenbetreibers gestützt werden kann. Da es für die Auslegung des Begriffs des „berechtigten“ Interesses derzeit jedoch weder eine gefestigte Rechtsprechung, noch nähere Anhaltspunkte von Seiten des Gesetzgebers gibt, kann eine Garantie hierfür an dieser Stelle noch nicht gegeben werden. Nichtsdestotrotz sprechen sehr starke Argumente dafür, dass auch ohne ausdrückliche Einwilligung von Seiten der Nutzer, der Einsatz eines Analysetools durch Stützung auf ein berechtigtes Interesse des Webseitenbetreibers gerechtfertigt werden kann.

Im Folgenden soll der Einsatz des Webanalysetools Matomo erläutert werden. Schließlich werden Hinweise gegeben, wie die Software eingestellt werden sollte, um den Interessen der Nutzer am Schutz ihrer personenbezogenen Daten Rechnung zu tragen, damit eine Berufung auf ein berechtigtes Interesse des Webseitenbetreibers statthaft erscheint.

III. Datenkontrolle durch Matomo (ehemals PIWIK)

Die meisten Anbieter von Webanalysetools speichern die Daten auf ihren eigenen Servern. So verfahren auch große Anbieter, wie Google Analytics oder Adobe Analytics. Rufen Nutzer eine Webseite auf, die durch eine solche Software überwacht wird, so wird deren IP-Adresse zusammen mit weiteren personenbezogenen Daten (meist unter Einsatz von Cookies) an die Anbieter der Webanalysetools übertragen. Nach Art. 5 DSGVO müssen personenbezogene Daten unter anderem in einer für den Betroffenen nachvollziehbaren Weise verarbeitet werden (Transparenzgebot). Eine Verarbeitung der Daten muss stets auf das für die Verarbeitung notwendige Maß reduziert bleiben (Datenminimierung) und die Sicherheit der verarbeiteten Daten muss von Seiten des Verantwortlichen gewährleistet sein (Integrität und Vertraulichkeit). Auch eine Weitergabe der Daten an Dritte stellt eine Datenverarbeitung dar. Diese sollte nur stattfinden, wenn sie zur Erreichung des Zwecks der Webanalyse zwingend erforderlich ist, Transparenz über die Weiterverarbeitung durch den Dritten geschaffen werden kann sowie die Sicherheit bei der Weitergabe der Daten gewährleistet ist. Oft sind diese Vorgaben durch Webseitenbetreiber bei der Weitergabe an Dritte schwer zu erfüllen. Vor diesem Hintergrund ist es ratsam, eine Datenanalyse auf den eigenen Servern stattfinden zu lassen.

Auf diese Weise behält der Webseitenbetreiber selbst die volle Kontrolle über die Verarbeitung der personenbezogenen Nutzerdaten. Eine solche Möglichkeit bietet die Open-Source Software Matomo. Bereits im März 2011 wurde deren Einsatz für die Webanalyse vom Unabhängigen Landeszentrum für Datenschutz in Schleswig-Holstein (ULD) empfohlen.

IV. Datenschutzrechtskonforme Einstellung des Tools

1. IP-Anonymisierung

Im Rahmen der Webanalyse werden auch die IP-Adressen der Nutzer beim Aufruf der Webseite gespeichert. Die IP-Adressen können von der Software bestimmten geographischen Regionen zugeordnet werden. Auf diese Weise gewinnen Webseitenbetreiber Hinweise über die Herkunft ihrer Nutzer und die Reichweite, die sie durch ihr Webangebot generieren. Allerdings sind IP-Adressen, nach aktueller Rechtsprechung des BGH, als personenbezogene Daten anzusehen,[2] was zur Folge hat, dass datenschutzrechtliche Normen Beachtung finden müssen. Der Personenbezug entsteht dadurch, dass der Internet-Service-Anbieter stets eine Zuordnung der aktuell genutzten IP-Adresse zu einem Kunden herstellen und somit der Anschlussinhaber ermittelt werden kann. Dies ist jedoch nur solange möglich, wie die IP-Adresse des aufrufenden Systems in ihrer vollen Länge verfügbar ist. Werden Teile der IP-Adresse gelöscht oder unkenntlich gemacht, so spricht man von einer „IP-Maskierung“. Eine maskierte IP-Adresse kann nicht mehr auf den Anschlussinhaber zurückgeführt werden. Ein Personenbezug ist dann nicht mehr gegeben. Nach einem Test des ULD hat die Maskierung der IP-Adresse auch keine Auswirkungen auf die Analyse der Herkunftsländer der Webseitenbesucher. Webseitenbetreibern ist daher zu raten, die IP-Adressen vor der Speicherung in die Datenbank zu maskieren. Dies gelingt bei Matomo durch die Funktion „AnonymizeIP“, welche unter dem Punkt „Administration › Privacy“ zu finden ist. Um einen Ausgleich zwischen dem Interesse des Webseitenbetreibers an der Herkunft seiner Nutzer und dem Interesse der Nutzer am Schutz ihrer personenbezogenen Daten zu schaffen, sollte die Hälfte der IP-Adresse maskiert werden. Dies entspricht auch der Empfehlung des ULD.

2 Zum Urteil des BGH bezüglich des Personenbezugs von IP-Adressen, siehe Mörike, BGH bestätigt: IP-Adressen sind personenbezogene Daten, in: DFN Infobrief Recht 09/2017.

2. Automatisierte Datenlöschung

Nach Art. 6 Abs. 1 lit. f DSGVO ist nur die für die Verfolgung der Interessen erforderliche Datenverarbeitung gerechtfertigt. Soweit also die Daten für die Zwecke der Webanalyse nicht mehr benötigt werden, müssen diese gelöscht werden. Dies gilt jedoch nur soweit die gespeicherten Daten weiterhin personenbezogene Daten der Nutzer enthalten. Sind die IP-Adressen bereits maskiert und enthalten die Datensätze keine weiteren Informationen, die eine Identifizierung der aufrufenden Nutzer ermöglichen würde, so ist, zumindest aus datenschutzrechtlichen Gründen, eine Löschung der Daten nicht erforderlich. Rückschlüsse auf den Nutzer können jedoch in Einzelfällen auch durch andere Daten als die IP-Adresse des Nutzers gezogen werden. Auch diese Daten können in die Analysedaten einfließen. Daher können sich Webseitenbetreiber manchmal nicht sicher sein, dass die erstellte Datenbank frei von jedem Personenbezug ist. In diesen Fällen ist eine automatisierte Löschung der Datensätze ratsam. Pauschale Angaben darüber, wann die Daten zu löschen sind, können nicht gemacht werden. Eine Löschung hat zu erfolgen, sobald die Daten für die Zwecke der Webanalyse nicht mehr erforderlich sind. Matomo selbst empfiehlt hierfür eine Löschfrist von 3-6 Monaten. Diese Angaben können als grober Richtwert dienen. Die Einstellung zur automatisierten Löschung der Daten findet sich unter „Administration › Privacy › Delete old visitor logs from database“.

3. Widerspruchsmöglichkeiten

Dem Nutzer kann die Möglichkeit eingeräumt werden, der Verarbeitung seiner personenbezogenen Daten zu Zwecken der Webanalyse zu widersprechen. Zwingend vorgeschrieben ist dies gem. Art. 21 DSGVO, im Falle der Datenverarbeitung auf Grundlage des Art. 6 Abs. 1 lit. f DSGVO, nur für diejenigen Fälle, in denen sich die Gründe hierfür aus der besonderen Situation des Nutzers ergeben oder die verarbeiteten Daten für Zwecke der Direktwerbung genutzt werden. Da jedoch unklar bleibt, in welchen Fällen Nutzer sich in einer besonderen Situation befinden und im Rahmen der Interessensabwägung der Schutz der personenbezogenen Daten der Nutzer möglichst weitreichend berücksichtigt werden sollte, ist es ratsam, den Nutzern beim Einsatz von Webanalysetools stets eine Widerspruchsmöglichkeit einzuräumen. Matomo bietet hierfür eine Lösung über einen „Opt-Out-Cookie“ an. Dieser

Cookie wird auf dem Rechner des Nutzers gespeichert. In der Folge wird bei weiteren Seitenaufrufen des betroffenen Nutzers die Information übertragen, dass eine Speicherung seiner Daten für Analysezwecke nicht gewünscht ist. Die Daten des Nutzers werden demensprechend nicht in die Datenbank aufgenommen. Die Möglichkeit zum Setzen dieses Cookies wird durch Implementierung eines „iFrames" auf der Webseite ermöglicht. Dieses wird als Fenster auf der zu analysierenden Webseite dargestellt. Der Webseitenbetreiber kopiert hierzu einen HTML-Code, der sich unter „Administration › Privacy" findet, an die gewünschte Stelle seiner Webseite. Diese sollte für die Nutzer leicht auffindbar sein. Es empfiehlt sich daher eine prominente Platzierung in der Datenschutzerklärung. Der Nutzer kann dann durch einen einfachen Klick das Setzen des Opt-Out-Cookies veranlassen.

V. Fazit

Auch Hochschulen und Forschungseinrichtungen haben ein berechtigtes Interesse an der Analyse der Besucherdaten ihrer Webseitenauftritte, um deren Funktionsfähigkeit und Nutzerfreundlichkeit zu verbessern. Nach Rechtslage ab dem 25. Mai 2018 ist ein Einsatz von Analysetools aber nur dann sicher gerechtfertigt, wenn eine ausdrückliche vorherige Einwilligung der Webseitenbesucher vorliegt. Dies ist dem Umstand geschuldet, dass die Abwägung des berechtigten Interesses des Webseitenbetreibers gegen das Interesse der Nutzer derzeit kaum rechtssicher vorgenommen werden kann. Eine diesbezügliche Klärung durch die Regelungen der E-Privacy-Verordnung wäre wünschenswert. Bis dahin bleibt eine Auslegung des Begriffs durch die Rechtsprechung abzuwarten.

Sowohl der Entwurf zur E-Privacy-Verordnung als auch das derzeit noch geltende deutsche Recht, mit seinem vergleichsweise hohen Datenschutzstandard, ermöglichen die Webanalyse auch ohne vorherige Einwilligung der Nutzer, soweit bestimmte Voraussetzungen erfüllt sind. Es sprechen daher gute Argumente dafür, dass auch nach Geltung der DSGVO und vor Einführung der E-Privacy-Verordnung eine Webanalyse mit Matomo ohne vorherige Einwilligung gerechtfertigt ist, soweit die IP-Adressen der Nutzer maskiert, die Daten sobald wie möglich gelöscht werden und eine Widerspruchsmöglichkeit in Form eines Opt-Out-Cookies eingeräumt wird.

Her damit!

Europäischer Gerichtshof qualifiziert Antworten eines Prüflings in einer berufsbezogenen Prüfung und die dazugehörigen Anmerkungen des Prüfers als personenbezogene Daten

von Franziska Leinemann

Mit Urteil vom 20.12.2017 (Rechtssache C-434/16) ordnet der Europäische Gerichtshof (EuGH) schriftliche Antworten eines Prüflings in einer berufsbezogenen Prüfung und die dazugehörigen Anmerkungen des Prüfers als personenbezogene Daten im Sinne von Artikel 2 Buchstabe a) der RL 95/46/EG ein. Die Konsequenz dieser Einordnung ist, dass dem Prüfling ein datenschutzrechtliches Auskunftsrecht zusteht. Die Entscheidung des EuGH ist auch für die Datenschutz-Grundverordnung (DSGVO), welche ab dem 25.05.2018 gilt, von Bedeutung.

I. Hintergrund

Gemäß Artikel 2 Buchstabe a) der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (RL 95/46/EG) bezeichnet der Ausdruck „personenbezogene Daten" alle Informationen über eine bestimmte oder bestimmbare natürliche Person („betroffene Person"). In Zweifelsfragen entscheidet der EuGH über die Auslegung von Begriffen, die auf eine Richtlinie zurückgehen.

Eine Richtlinie – so auch die RL 95/46/EG – muss in nationales Recht umgesetzt werden. Dies ergibt sich aus Artikel 288 Absatz 3 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV). Gemäß Artikel 288 Absatz 3 AEUV ist die Richtlinie für jeden Mitgliedstaat, an den sie gerichtet wird, hinsichtlich des zu erreichenden Ziels verbindlich, überlässt jedoch den innerstaatlichen Stellen die Wahl der Form und der Mittel. Die Mitgliedsstaaten haben die Richtlinie durch nationale Datenschutzgesetze umgesetzt. Ab dem 25.05.2018 gilt unmittelbar die neue Datenschutz-Grundverordnung (DS-GVO), die im Gegensatz zu einer Richtlinie keiner Umsetzung durch nationale Gesetze bedarf. Alle datenschutzrechtlichen Streitigkeiten, die vor diesem Datum beginnen, sind wie bisher nach der RL 95/46/EG und den jeweiligen nationalen Datenschutzgesetzen zu bestimmen. Der vorliegende Fall begann im Jahr 2009 in Irland und ist daher nach irischem Datenschutzrecht und der europäischen Datenschutz-Richtlinie zu beurteilen.

II. Entscheidung des EuGH

1. Sachverhalt

Der Kläger Peter Nowak war Trainee Accountant (Wirtschaftsprüfer/Steuerberater in Ausbildung). Mehrfach fiel er durch die Prüfung „Strategic Finance und Management Accounting", die das Institute of Chartered Accountants of Ireland (irische Berufsorganisation für Wirtschaftsprüfer/Steuerberater (CAI)) abnimmt. Auch im Herbst 2009 fiel Peter Nowak durch die genannte Prüfung. Er reichte daraufhin Beschwerde ein, um das Ergebnis anzufechten. Diese Beschwerde wurde im März 2010 zurückgewiesen. Peter Nowak stellte sodann einen Antrag auf Auskunft über alle ihn betreffenden personenbezogenen Daten, die das CAI besitzt. Diesen Antrag stützte er auf das irische Datenschutzgesetz, welches die RL 95/46/EG in das irische Recht umsetzt.

Das CAI verneinte, Peter Nowak die Prüfungsarbeit auszuhändigen, da es sich hierbei nicht um personenbezogene Daten im Sinne des irischen Datenschutzgesetzes handele.
Peter Nowak trat nun an den Datenschutzbeauftragen heran.

Dieser schloss sich jedoch der Auffassung des CAI an, dass es sich vorliegend nicht um personenbezogene Daten handele. Am 01.07.2010 reichte Peter Nowak eine formelle Beschwerde beim Datenschutzbeauftragten ein. Am 21.07.2010 informierte der Datenschutzbeauftragte Peter Nowak, dass er die Beschwerde geprüft habe, ihr jedoch nicht weiter nachgehen werde.

Peter Nowak erhob gegen diese Entscheidung des Datenschutzbeauftragten Klage. Der Circuit Court (Bezirksgericht) schloss sich jedoch dem Datenschutzbeauftragten an, dass es sich nicht um personenbezogene Daten handele. Das Urteil des Circuit Court wurde vom High Court (Hoher Gerichtshof) bestätigt; das Urteil des High Court sodann vom Court of Appeal (Berufungsgericht). Der Supreme Court (Oberster Gerichtshof) zweifelte jedoch an dieser Einschätzung und legte aus diesem Grund dem EuGH Fragen zur Vorabentscheidung vor, um zu klären, ob „die schriftlichen Antworten eines Prüflings in einer berufsbezogenen Prüfung und etwaige Anmerkungen des Prüfers dazu“ (s. EuGH, Urteil vom 20.12.2017 – Rechtssache C-434/16, Randnummer 27) als „personenbezogene Daten“ im Sinne von Artikel 2 Buchstabe a der RL 95/46/EG zu qualifizieren sind.

2. Urteil

Der EuGH führt zunächst aus, dass ein Prüfling in einer berufsbezogenen Prüfung eine natürliche Person sei. Diese könne entweder anhand ihres Namens oder einer Kennnummer identifiziert werden. Nicht entscheidend sei insoweit, dass der Prüfer den Prüfling während der Korrektur gegebenenfalls nicht identifizieren kann. Vielmehr sei ausreichend, dass die CAI den Prüfling identifizieren kann (s. hierzu auch Mörike, BGH bestätigt: IP-Adressen sind personenbezogene Daten, DFN-Infobrief Recht 09/2017 und Sydow, Speichern ist relativ?, DFN-Infobrief Recht 12/2016).

Der EuGH stellt weiter fest, dass der Ausdruck „personenbezogene Daten“ im Sinne der RL 95/46/EG weit zu verstehen sei. Diese spiegele sich auch in Artikel 2 Buchstabe a) RL 95/46/EG wider („alle Informationen“). Insbesondere seien nicht nur „sensible oder private Informationen“ (s. EuGH, Urteil vom 20.12.2017 – Rechtssache C-434/16, Randnummer 34) erfasst.
Es handele sich um eine Information über eine natürliche Person, „wenn die Information aufgrund ihres Inhalts, ihres Zwecks oder ihrer Auswirkungen mit einer bestimmten Person verknüpft“ (s. EuGH, Rechtssache C-434/16, Randnummer 35) sei. Dies sei bei Antworten eines Prüflings in einer berufsbezogenen Prüfung der Fall. Unter anderem könnten Rückschlüsse auf die fachliche Eignung des Prüflings gezogen werden. Auch die Anmerkungen des Prüfers seien als Informationen über den Prüfling zu qualifizieren.

Eine andere Bewertung sei auch nicht damit zu rechtfertigen, dass dem Prüfling somit ein Recht auf Auskunft gemäß Artikel 12 Buchstabe a) RL 95/46/EG und ein Recht auf Berichtigung gemäß Artikel 12 Buchstabe b) RL 95/46/EG zustünden. Das Recht auf Berichtigung gemäß Artikel 12 Buchstabe b) RL 95/46/EG sei unverkennbar nicht so zu verstehen, dass der Prüfling falsche Antworten nachträglich verbessern könne.

Abschließend merkt der EuGH an, dass die Prüfungsfragen als solche nicht als personenbezogene Daten des Prüflings einzuordnen seien.

III. Fazit und Konsequenzen für wissenschaftliche Einrichtungen

Wie eingangs bereits erwähnt, gilt ab dem 25.05.2018 die DS-GVO. Sie gilt gemäß Artikel 288 Absatz 2 AEUV unmittelbar in jedem Mitgliedstaat. Auf die nationalen Datenschutzgesetze kommt es dann nicht mehr an. Gemäß Artikel 4 Nummer 1 DS-GVO bezeichnet der Ausdruck „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen. Artikel 4 Nummer 1 DS-GVO weicht zwar in sprachlicher Hinsicht geringfügig von Artikel 2 Buchstabe a RL 95/46/EG ab. Auch der Ausdruck „personenbezogene Daten“ im Sinne von Artikel 4 Nummer 1 DS-GVO ist jedoch denkbar weit auszulegen. Wenngleich der EuGH vorliegend noch zu Artikel 2 Buchstabe a) RL 95/46/EG urteilt, sollte dieses Ergebnis auch unter Geltung der DS-GVO berücksichtigt werden. Es ist nicht zu erwarten, dass der EuGH den vorliegenden Fall unter Berücksichtigung der DS-GVO anders entscheiden würde. Auch die DS-GVO beinhaltet mit ihrem Artikel 15 ein Recht auf Auskunft. Wissenschaftliche Einrichtungen, die berufsbezogene Prüfungen abnehmen, sind jetzt und in Zukunft datenschutzrechtlich verpflichtet, den Prüflingen auf Nachfrage Auskunft über ihre Antworten und die Anmerkungen des Prüfers zu geben.

Impressum

Der DFN-Infobrief Recht informiert über aktuelle Entwicklungen in Gesetzgebung und Rechtsprechung und daraus resultierende mögliche Auswirkungen auf die Betriebspraxis im Deutschen Forschungsnetz.

Herausgeber

Verein zur Förderung eines Deutschen Forschungsnetzes e. V.
DFN-Verein
Alexanderplatz 1, D-10178 Berlin
E-Mail: DFN-Verein@dfn.de

Redaktion

Forschungsstelle Recht im DFN
Ein Projekt des DFN-Vereins an der WESTFÄLISCHEN WILHELMS-UNIVERSITÄT, Institut für Informations-, Telekommunikations- und Medienrecht (ITM), Zivilrechtliche Abteilung
Unter Leitung von Prof. Dr. Thomas Hoeren
Leonardo-Campus 9
D-48149 Münster
E-Mail: recht@dfn.de