Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Vortrag

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Prof. Ulrich Kelber

Die Bedeutung von Datenschutz im Open Source Bereich

„Volle Transparenz“ – Open Source als Vertrauensanker

bei
Free and Open Source Software Conference (FrOSCon) e.V.
Hochschule Bonn Rhein Sieg in Sankt Augustin, 22. August 2020

Es gilt das gesprochene Wort

I. [Einleitung]

Guten Morgen zusammen,

in diesem Jahr findet die FrOSCon wegen der COVID-19-Pandemie online statt. In diesem Sinne auch von mir ein herzliches Willkommen in dieser neuen Normalität. Digitale Veranstaltungsformate – wie die Konferenz heute – gehören in Zeiten des Corona-Virus mittlerweile zu unserem alltäglichen Leben. Auch ich persönlich hatte in den vergangenen Monaten nur ganz wenige externe physische Treffen. Und die fühlten sich tatsächlich fast schon ungewohnt an. Händeschütteln in Filmen kommt mir ähnlich altertümlich vor wie ein Hofknicks.

Eines ist sicher: Corona hat in der breiten Gesellschaft die Erfahrungen mit Digitalisierung stark verändert. Die Pandemie zeigte uns sehr deutlich, wie wichtig die Digitalisierung für uns alle ist. In den vergangenen Monaten des „social distancing“ haben uns vielfältige digitale Formate unterstützt und ein – wenn auch virtuelles – Miteinander überhaupt erst ermöglicht.

Ob mobile Arbeit, eLearning oder viele andere digitale Kollaborationen. Digitalisierung schafft völlig neue, offene Partizipationsmöglichkeiten. Das ist eine enorme Chance. Niemals war es einfacher, live an noch so entfernten und exklusiven Veranstaltungen teilzunehmen. Und auch das Angebot wächst. Ich bin sehr gespannt inwieweit dieser Trend nach der Pandemie anhalten wird.

Auch die deutsche Corona-Warn-App hat viele Menschen überzeugt. Obgleich es hier gerade in den vergangenen Wochen harsche Kritik an der technischen Umsetzung gab. Wie Sie vielleicht wissen, stand mein Haus dem Entwicklungskonsortium mit Blick auf den Datenschutz beratend zur Seite.

Insgesamt kann man sagen, wir haben die Situation auch Dank der Digitalisierung bisher in dieser Weise gemeistert.

Wie kommt hier jetzt Free and Open Source Software ins Spiel?

Die Pandemie hat Fragen nach Softwarearchitekturen und Kriterien für eine sinnvolle Auswahl und Beschaffung von Software neu entfacht. Der Einsatz von Free and Open Source Software hat hierbei eine ganz besondere Rolle gespielt. Hierauf gehe ich gleich noch detaillierter ein. Ich werde dabei der Einfachheit halber nur noch von Open Source sprechen. Der freiheitliche Gedanke der „Free“ Software schwingt bei meinen Überlegungen aber natürlich stets mit.

Für mich ist es heute bei Ihnen ein Heimspiel. Nicht nur, weil ich Bonner bin – und damit quasi Ihr Nachbar. Auch nicht, weil ich Informatiker bin.

Der Grund ist ein anderer: Sie und mich verbindet ein starkes Band:

Wir stehen gemeinsam für das Prinzip der Transparenz.

In meiner Funktion als Bundesbeauftragter bin ich auch Hüter der Informationsfreiheit, also Sachwalter für die Transparenz der öffentlichen Verwaltung. Transparenz ist aber selbstverständlich auch im Datenschutz ein ganz entscheidender Erfolgsfaktor. Denn die Beherrschbarkeit und Rechtmäßigkeit einer Datenverarbeitung setzt voraus, dass transparent wird, welche Daten in welcher Weise verarbeitet werden.

Gerne möchte ich für die heutige Diskussion einen Beitrag zur Bedeutung des Datenschutzes im Open Source Bereich beisteuern. Wie bedingen und befruchten sich also Datenschutz und Open Source?

Um direkt mit der Tür ins Haus zu fallen: Open Source hilft bei Fragen der Transparenz ungemein, ist nicht selten unbedingte Voraussetzung dafür. Deshalb ist Open Source nach meiner festen Überzeugung ein wichtiger Vertrauensanker für die Digitalisierung.

Lassen Sie mich ausführen, was ich damit konkret meine – und warum wir gut beraten sind, stärker auf Open Source Lösungen zu setzen.

II. Erstens: Open Source schafft Transparenz, Sicherheit und fördert so den Datenschutz

Aus datenschutzrechtlicher Sicht ist der Anspruch auf Transparenz ein grundsätzlich verbürgtes Recht. Er wird explizit in Art. 5 Abs. 1 a) der Datenschutzgrundverordnung genannt. Im Kern geht es darum, dass eine betroffene Person nachvollziehen können muss, wie die sie betreffenden personenbezogenen Daten verarbeitet werden.

Dieses Wissen ist die Basis für eine selbstbestimmte Entscheidung über die Datennutzung. Denn nur mit dieser Transparenz kann es gelingen, die Kontrolle über die Verwendung eigener (personenbezogener) Daten zu behalten. Und diese Kontrolle ist eine zwingende Voraussetzung für den effektiven Schutz der eigenen Daten.

In der Diskussion um das Für und Wider von Open Source Software ist das Thema Transparenz ein klares Pro-Argument für Open Source.

Denn der Quellcode der Software ist frei zugänglich. Die Idee eines für Jedermann einsehbaren und nachprüflich eingesetzten Quellcodes sorgt dafür, dass der Code das macht, was er soll – aber nicht mehr. Es würde in der Community vermutlich sehr schnell auffallen, wenn eine Software weitere, nicht beschriebene Funktionalitäten aufweisen würde. Hier lässt sich sicher der Vergleich zur „Schwarmintelligenz“ ziehen.

Die Nachprüfbarkeit vereinbarter Eigenschaften spielt bei Software also eine ganz herausragende Rolle. Ganz nach dem Motto „Vertrauen ist gut, Kontrolle ist besser“. Wird eine Software als Open Source Projekt entwickelt, erleichtert dies die Nachprüfbarkeit ungemein. Selbst dann, wenn derjenige, der eine Software einsetzen möchte nicht selbst über die notwendige Fachexpertise verfügt, könnte er unproblematisch externen Sachverstand zurate ziehen und mit einer Prüfung beauftragen.

Open Source generiert aber auch Mehrwerte mit Blick auf die IT-Sicherheit. Hier gilt das soeben Gesagte entsprechend: Weil der Quellcode für jedermann zugänglich ist, hat jeder die Möglichkeit, auf Probleme hinzuweisen und sie zu beseitigen. Sicherheitslücken werden so schnell offenbar. Die Entwicklung wird eben nicht exklusiv von einem Einzigen kontrolliert und gesteuert, sondern von einer „Community“.

Aus Sicht des Datenschutzes ist IT-Sicherheit eine unverhandelbare Grundvoraussetzung. Wenn Sie so wollen, sind IT-Sicherheit und Datenschutz unmittelbar miteinander verzahnt – zwei Seiten derselben Medaille. Denn IT-Sicherheit soll den Missbrauch, unberechtigten Zugang und die unberechtigte Nutzung personenbezogener Daten ausschließen. IT-Sicherheitsrisiken sind damit regelmäßig auch Datenschutzrisiken. Alle Mehrwerte für IT-Sicherheit kommen deshalb auch dem Datenschutz zugute.

III. Ein paar Worte zur datenschutzrechtlichen Haftung bei Open Source

Open-Source lebt gerade davon, dass zahlreiche Entwickler die Möglichkeit haben, die Software zu erhalten, weiterzuentwickeln und ihre eigenen Ergebnisse Dritten zugänglich zu machen. Wie Sie alle wissen, ist die Weiterverwertung, Vervielfältigung und Bearbeitung von Open Source aber natürlich nicht nach allen Open Source Lizenzen in gleicher Weise vorbehaltlos gestattet.

Vielmehr wird die Einräumung von Nutzungsrechten bei Open Source Software in aller Regel von bestimmten Voraussetzungen abhängig gemacht. Hier stehen u.a. verschiedene Lizenzmodelle mit unterschiedlichen Anforderungen an die Verwender zur Auswahl. Bei der Nutzung von Open Source sind deshalb durchaus verschiedene juristische Fallstricke zu beachten.

Ich wurde gebeten, kurz etwas zur datenschutzrechtlichen Haftung bei Open Source zu sagen.

Haftungsfragen sind immer Risikofragen, die als Damoklesschwert über Software-Unternehmen und Programmierern schweben. Um Ihren Erwartungshorizont direkt etwas abzuflachen: Eine pauschale Antwort auf alle Haftungsfragen bei Open Source kann ich hier natürlich nicht geben. Dies würde diesen Rahmen schlicht sprengen. Es wäre aber auch unlauter, weil auch die Haftungsfragen – wie immer im Recht – vom jeweiligen Einzelfall abhängen.

Lassen Sie mich dennoch ein paar ganz grundsätzliche Anmerkungen zur Frage machen. Ich möchte mich dabei insbesondere auf meine Domäne fokussieren, den Datenschutz.

Grundsätzlich ist der Normadressat des Datenschutzrechts in erster Linie der „Verantwortliche“. Er ist es, der die datenschutzrechtlichen Pflichten zu beachten hat. Und er ist es auch, an den sich die Datenschutzaufsichtsbehörden wenden, wenn es um die Überwachung und Durchsetzung der Datenschutzvorgaben geht.

Gesetzlich definiert ist der Verantwortliche als diejenige Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (das ist legaldefiniert in Art. 4 Nr. 7 der Datenschutzgrundverordnung).

Um es konkret auf den Fall von Softwarenutzung zu münzen:

Verantwortlich ist grundsätzlich derjenige, der über den Einsatz einer Software entscheidet. Das ist regelmäßig nicht der Entwickler bzw. Anbieter der Software, sondern z.B. der Arbeitgeber oder Arzt, der eine Software konkret auswählt und dann aufbauend hierauf einsetzt.

Nur wenn der Software-Anbieter selbst bei der Verarbeitung personenbezogener Daten involviert ist und hierbei eigene Zwecke verfolgt, kann auch er Verantwortlicher sein. Das mag im Cloud-Kontext häufiger der Fall sein. Auch hier agiert der Software-Anbieter dann aber in der Regel als „verlängerter Arm“ desjenigen, der die Software einsetzt. Er führt dann lediglich weisungsgebunden aus, was ihm aufgetragen wurde. Auch hier liegt dann keine Verantwortlichkeit im datenschutzrechtlichen Sinne vor, sondern eine Auftragsverarbeitung.

Um es nicht unnötig komplex zu machen: Wir können es also bei der Gleichung belassen, dass ein Verantwortlicher über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden können muss. Und dieser Verantwortliche ist es auch, der für die Datenschutzkonformität einstehen – konkret haften – muss.

Welche Rolle spielt hier nun aber Open Source? Open Source macht es dem Verantwortlichen grundsätzlich besser möglich, diese Abschätzung vorzunehmen. Hier kann ich mich nur wiederholen: Er kann sich selbst oder wenigstens mit Hilfe von Prüfsystem oder Experten bis auf die Quellcode-Ebene davon überzeugen, dass es keinen Datenabfluss gibt und die Daten nur entsprechend der erforderlichen Zwecke verarbeitet werden.

IV. Zweitens: Open Source schafft Vertrauen – die Corona-Warn-App als Blaupause

Open Source ist auch bei global agierenden Software-, IT- und Telekommunikationsunternehmen zu einer echten Handlungsoption avanciert. Ein Beispiel hierfür ist die Corona-Warn-App.

Tim Höttges bezeichnete sie als "Rockstar" unter den Apps. Nun ja, ein derart mondänes Leben führt die Corona-Warn-App sicher nicht. Insbesondere nicht nach der jüngsten Kritik an ihrer technischen Umsetzung, etwa mit Blick auf die Hintergrundaktualisierung. Aber vielleicht kommen wir jetzt an einen Punkt, an dem wir Open Source – um in Duktus der Deutschen Telekom zu bleiben – als „Gamechanger“ verstehen und einsetzen.

Lange wurde in Deutschland gerungen um die Ausgestaltung der Corona-App. In kaum einem anderen Softwaregroßprojekt wurden wichtige Designentscheidungen derart kontrovers in und mit der Öffentlichkeit diskutiert. Beispielsweise zu der Frage, ob ein zentraler oder dezentraler Systemansatz gewählt werden soll. Die Corona-Warn-App ist – das wird man unbestritten sagen können – bei Softwareprojekten der Bundesregierung ein Leuchtturm für transparente Softwareentwicklung.

Ein wesentlicher Baustein dieser Transparenz ist dabei sicherlich die Veröffentlichung des Quellcodes und der begleitenden Entwicklungsdokumentation der App. Gerade hier hat die Möglichkeit zur externen Prüfung stark zum Abbau von Misstrauen gegenüber dem Projekt beigetragen.

Ich sagte es bereits, mein Haus hat den Entwicklungsprozess im Rahmen der datenschutzrechtlichen Beratung begleitet. Datenschutz wurde bei der Corona-Warn-App von Anfang an mit betrachtet.

Im offenen aber auch kritischen Austausch mit den Entwicklern und dem Robert-Koch-Institut ist es uns dabei in nahezu allen Bereichen gelungen, auch im Detail datenschutzfreundliche Lösungen zu etablieren. Wo dies noch nicht möglich war, z.B. bei der externen Verifikationshotline, gehe ich fest davon aus, dass auch hier zeitnah Verbesserungen erreicht werden.

Bei der Begleitung des Projekts war es uns ein besonders wichtiges Anliegen, dass - ganz im Sinne des Open-Source Gedankens - die Datenschutzdokumentation veröffentlicht wird und damit einer Überprüfung durch die Zivilgesellschaft offen steht. Diese Veröffentlichung schafft auch Mehrwerte für interessierte Nutzerinnen und Nutzer, die sich so umfassender informieren können, als dies durch eine einzelne Datenschutzerklärung möglich wäre. Die offene Kommunikation von Datenschutzrisiken und korrespondierender Schutzmaßnahmen sowie die Erläuterung von Designentscheidungen haben so den wesentlichen Beitrag zur Vertrauensbildung geleistet.

Ich bin auch aus einem anderen Grund sehr dankbar für den Erfolg der Corona-Warn-App. Denn sie zeigt, dass das Image des Datenschutzes in der Vergangenheit völlig unbegründet negativ besetzt war.

Allzu oft wurde mit Datenschutz ein „Bremsschuh für Innovationen“ assoziiert. Datenschutz bremse technologischen Fortschritt und wirtschaftliche Entwicklung oder schrecke Investoren ab, so die immer wieder vorgetragene Position. Verwiesen wird hier gerne auf die weit entwickelten Digitalökonomien in China oder den USA. Ihr Vorsprung im Bereich der digitalen Technologien wird als quasi „uneinholbar“ beschrieben. Auch und gerade wegen laxerer Datenschutzvorgaben.

Ich frage Sie aber: Wie sollte eine verantwortungsbewusste und sinnvolle technologische Weiterentwicklung ohne Datenschutz aussehen? Unser gemeinsames Ziel muss es doch sein, den Rückzug in die Privatheit selbstbestimmt zu ermöglichen und gleichzeitig die Chancen der Digitalisierung zu nutzen. Wir müssen die Privatsphäre schützen, auch und gerade um einen Freiraum zur unbeobachteten persönlichen Entfaltung zu belassen. Genau deshalb ist mir wichtig, bei allen Digitalisierungstrends immer wieder an die Bedeutung der „Privatheit“ zu erinnern.

Das sehe ich als meinen ganz persönlichen Auftrag – aber auch als unsere gemeinsame, gesamtgesellschaftliche Aufgabe – an.

Es ist doch absurd, dass hier in Deutschland, wo wir Erfahrung mit Datenschutz haben und diesen aus den Grundrechten ableiten, von Wirtschaftsverbänden und Politik über Datenschutz als Wettbewerbshindernis gejammert wird, während in den USA Firmen zunehmend – berechtigt oder unberechtigt – mit Datenschutz für sich werben?

Die Corona-Warn-App zeigt, dass Datenschutz kein Innovationshemmnis ist. Genau das Gegenteil ist der Fall, wie die Downloadzahlen der App recht deutlich zeigen. Und genau dieser Imagewechsel muss nun in Wirtschaft und Gesellschaft stärker verankert werden: Datenschutz stellt einen wichtigen Erfolgsfaktor dar.

Denn die App basiert auf einer rein freiwilligen Nutzung. Niemand wird gezwungen, die App zu verwenden. Wegen dieser Freiwilligkeit wird das Vertrauen in den Datenschutz zum Zünglein an der Waage für den Erfolg der App. Es würde wohl kaum jemand die App freiwillig nutzen, wenn er befürchten müsste, dass mit den personenbezogenen Daten Schindluder getrieben wird.

Dennoch ist es natürlich wichtig, die Entwicklungen hier wachsam weiter zu beobachten: Einer eventuellen Verpflichtung zur Nutzung oder gar zum Vorzeigen der App im Sinne eines Risikonachweises durch öffentliche Stellen wie nicht-öffentliche Stellen gilt es auch in Zukunft entschieden entgegen zu treten.

Ich meine, wir sollten dazu beitragen, Datenschutz zu einem Wettbewerbsvorteil, einem besonderem Qualitätsmerkmal in Deutschland und Europa zu entwickeln. Dann wird Datenschutz zu einem wichtigen Differenzierungsmerkmal im globalen Markt.

Die öffentliche Hand muss den Erfolg der Corona-Warn-App als Chance begreifen und darf bei Software/Projekten, die mit öffentlichen Mitteln entstehen, nicht mehr hinter diesen Goldstandard zurückfallen. Außerdem muss man sich im Zweifelsfall für die datenschutzfreundlichere Architektur entscheiden.

V. Drittens: Open Source führt zu mehr Souveränität

Lassen Sie mich noch ein paar Worte zum Thema „Digitale Souveränität“ verlieren. Die „digitale Souveränität“ ist als politische Zielvorstellung mittlerweile etabliert. Böse Zungen behaupten, es würde als „Buzzword“ in der politischen Kommunikation verwandt, ohne dass es eine konturenscharfe Definition gäbe. Richtig hieran ist, dass nicht einhellig beantwortet wird, was denn nun unter dieser „digitalen Souveränität“ konkret verstanden wird – und wie sie umgesetzt werden soll.

Im Kern geht es immer wieder darum, die Abhängigkeiten zu einzelnen IT und Software-Anbietern zu verringern und einer wachsenden Technologieabhängigkeit entgegenzuwirken. Souverän sein zielt darauf ab, seine Rolle in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können. Ein souveräner datenschutzrechtlich Verantwortlicher kann frei entscheiden, welche Handlungsoptionen er wählt, um die Datenschutzanforderungen sicher umzusetzen. Als Einzelperson, als Organisation, als Staat oder Staatengemeinschaft.

Die Beratungsgesellschaft PWC hat Ende 2019 für die Bundesverwaltung eine strategische Marktanalyse zur Reduzierung von Abhängigkeiten zu einzelnen Software-Anbietern vorgelegt.[1] Gezeigt wurde, dass die Bundesverwaltung in einem kritischen Maße von einzelnen Anbietern abhängig ist. Hier geht es natürlich besonders um Produkte eines Anbieters aus Redmond. Es steht also nicht wirklich gut um die digitale Souveränität der deutschen Verwaltung.

Auch hier kann Open Source einen wichtigen Beitrag leisten. Denn Open Source macht es leichter möglich, sich auch über hochkomplexe Software einen sicheren Eindruck zu verschaffen. Denn ein öffentlich verfügbarer und überprüfbarer Quellcode macht die Prüfung auch an dieser Stelle sehr viel transparenter. Es geht also abermals um Kontrollmöglichkeiten, ohne die ein selbstständiges und selbstbestimmtes Handeln nicht möglich ist.

[1] Abrufbar unter https://www.cio.bund.de/SharedDocs/Publikationen/DE/Aktuelles/20190919_strategische_marktanalyse.pdf?__blob=publicationFile

Die Nutzung von offenen Standards trägt hier natürlich dazu bei, die Überprüfbarkeit und Kontrolle zu erleichtern. Dies betrifft Systemsoftware und insbesondere Datenformate, aber auch Software und Datenbanken, die auf Softwareplattformen aufsetzen. Denn die Transparenz von offenen Standards führt auch an dieser Stelle zu einer naturgemäß einfacheren Kontrollierbarkeit. Offene Standards sind zudem geeignet, unerwünschte Lock-in-Effekte zu vermeiden. Offene Schnittstellen, Standards und Software erhöhen in diesem Sinne die eigene digitale Souveränität.

Open Source ist wegen seiner Quelloffenheit aber auch besonders nachhaltig. Denn selbst, wenn der bisherige Anbieter einer Software insolvent sein sollte, wäre der Betrieb nicht gefährdet und könnte von einem Dritten recht friktionsfrei weitergepflegt werden.

VI. [Ausklang]

Lassen Sie es mich so zusammenfassen:

Open Source ist kein Dogma. Auch mit proprietärer Software können natürlich alle datenschutzrechtlichen Anforderungen erfüllt werden. Die inhärente Transparenz von Open Source führt aber typischerweise zu einer einfacheren und möglicherweise besseren Nachweisbarkeit der Datenschutzkonformität. Open Source hat also das Potenzial, zu einem echten Vertrauensanker der Digitalisierung zu werden.

Lassen Sie uns alle gemeinsam daran arbeiten, diesen Vertrauensanker weiter zu fördern und auszubauen.

Ich danke Ihnen für Ihre Aufmerksamkeit.