www.betriebs-berater.de

Betriebs Berater

BB

42 | 2019

Recht ... Wirtschaft ... Steuern ... Stablecoins ... IFRS ... Datenschutz ... Recht ... Wirtschaft ...

14.10.2019 | 74. Jg.
Seiten 2433–2496

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

Philipp M. Kühn, RA, und Neil C. Weaver, LL.B., RA

DSGVO vs. AGILE? – Prozess- und Produktgestaltung in agilen Projekten unter datenschutzrechtlichen Aspekten

Agile Methoden nehmen nicht nur in IT-Projekten, sondern auch in der internen Arbeitsorganisation immer mehr Bedeutung ein. Neben vielen anderen rechtlichen Herausforderungen müssen dabei auch die geltenden datenschutzrechtlichen Vorschriften in Bezug auf die agile Entwicklung und die agile Arbeitsorganisation berücksichtigt werden. Auf den ersten Blick besteht ein Konflikt mit den vermeintlich starren Vorschriften der Datenschutzgrundverordnung (DSGVO) und den anwendbaren datenschutzrechtlichen Vorschriften. Ob und inwiefern die Verarbeitung von personenbezogenen Daten in agilen Projekten im Einzelnen eine Rolle spielt und wie im Rahmen von agiler Software-Entwicklung datenschutzrechtliche Vorgaben, wie zum Beispiel die Grundsätze „Privacy by Design" und „Privacy by Default", umgesetzt werden können, ist jedoch nicht ohne Weiteres herzuleiten. Daher erläutert dieser Beitrag zunächst die rechtlichen Rahmenbedingungen (I.), um dann zu untersuchen, wie diese im Rahmen eines iterativen Vorgehens umgesetzt werden können (II.) und im Anschluss daran die Frage aufzulösen, welchen Mehrwert ein datenschutzrechtlich geprägtes agiles Mindset (III.) in sich birgt.

I. Rechtliche Rahmenbedingungen agiler Projekte

Auch wenn agile Methoden[1] und das agile Mindset von dem Grundsatz geprägt sind, dass Individuen und Zusammenarbeit wichtiger sind als Prozesse,[2] sind dennoch gerade im deutschen Rechtsraum unterschiedliche rechtliche Rahmenbedingungen (auch) bei der agilen Software- und Produktentwicklung zu berücksichtigen. Neben der vertragstypologischen Einordnung eines agilen Entwicklungsvertrages,[3] die eher vor der Umsetzung eine Rolle spielt, sind dies Anforderungen aus dem Datenschutz- und dem Arbeitsrecht, die es hier mit zu betrachten gilt. Im Rahmen der datenschutzrechtlichen Betrachtung eines agilen Projektes kann grundsätzlich zwischen den datenschutzrechtlichen Anforderungen an die Arbeitsorganisation auf der einen Seite und denen an die eigentliche Entwicklung und Software auf der anderen Seite unterschieden werden. Bei Letzterer ist insbesondere auch der Arbeitnehmerdatenschutz zu beachten.

1. Datenschutz im Rahmen der Entwicklung

Neben den allgemeinen Regelungen der DSGVO sind im Rahmen der Entwicklung insbesondere die in Art. 25 DSGVO verankerten Grundsätze des „Privacy by Design" (Datenschutz durch Technikgestaltung, Abs. 1) und „Privacy by Default" (Datenschutz durch datenschutzfreundliche Voreinstellungen, Abs. 2) zu berücksichtigen.

Die DSGVO geht davon aus, dass der durchschnittliche Nutzer nur über beschränkte IT-Kenntnisse verfügt und deshalb selbst keine Sicherheitsmaßnahmen ergreifen kann, um den Schutz seiner personenbezogenen Daten zu gewährleisten.[4] Daher ist es Aufgabe des Herstellers, für die Umsetzung der Grundsätze des Privacy by Design und Privacy by Default Sorge zu tragen, die Software so zu entwickeln, dass sie schon aufgrund ihrer Gestaltung die Grundsätze berücksichtigt und damit auch in allen andere Belangen „DSGVO compliant" ist, also auch die übrigen datenschutzrechtlichen Anforderungen der DSGVO umgesetzt sind.

Der Europäische Datenschutzbeauftragte gibt hierzu vor, dass sämtliche Datenverarbeitungen auf einem „design project" fußen und dabei der Schutz personenbezogener Daten zur Zielvorgabe gemacht werden sollte.[5] Hierbei sollen Datenverarbeitungen im Sinne der Datensparsamkeit und Zweckgerichtetheit i. S. d. Art. 25 Abs. 2 DSGVO nur in den Fällen erfolgen, in denen diese aus Sicht der Betroffenen erwartungsgemäß zur Zweckerreichung notwendig sind.[6] Beispielsweise soll eine Carsharing-App die Nutzer-Standortdaten nur für das eigene Leistungsangebot verwenden und diese Daten gerade nicht an Drittanbieter zu Marketingzwecken weiterleiten.[7] Es sollen konkrete technische Vorschläge zur datenschutzkonformen Umsetzung der Vorgaben herangezogen werden. Hier wird die Pseudonymisierung[8] von Daten- oder ganzen Datensätzen genannt.

Im Rahmen des „design projects" sollen auch die nachfolgenden Pflichten des späteren Betreibers als Verantwortlicher (bspw. Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO, Nachweispflicht für erteilte Einwilligungen, Dokumentationspflichten bzgl. Verfahrensverzeichnisse und der Datenschutzfolgenabschätzung nach Art. 35 DSGVO[9]) einfließen.

Schließlich müssen sich Softwarehersteller und deren Entwickler auch regelmäßig über die Entwicklung neuer technischer Standards informieren, da diese im Rahmen der Grundsätze des Art. 25 DSGVO

1 An dieser Stelle soll betont werden, dass „Agile" und „Scrum" nicht gleichzusetzen sind, sondern dass Scrum lediglich eine der Ausprägungen des agilen Verfahrens darstellt, vgl. hierzu bspw. *Denning*, https://www.forbes.com/sites/stevedenning/2019/08/25/why-the-future-of-agile-is-bright/#2b757e8e2968 (Abruf: 16.9.2019).

2 Vgl. hierzu die Ausführungen bei *Kühn/Ehlenz*, CR 2018, 139, 142 sowie http://agilemanifesto.org (Abruf: 16.9.2019).

3 S. hierzu mit ausführlicher Einführung und Besprechung der verschiedenen Ansätze *Kühn/Ehlenz* (Fn. 2), sowie *Kühn*, ReThinkinglaw 5/2019, 67 ff.

4 *Schaar*, Privacy by Design, https://www.bfdi.bund.de/SharedDocs/Publikationen/%22PrivacyByDesign%22.html (Abruf: 16.9.2019).

5 EDPS, Opinion 5/2018, abrufbar unter https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf (Abruf: 16.9.2019), S. 6.

6 EDPS (Fn. 5), S. 7.

7 EDPS (Fn. 5), S. 6.

8 Vgl. zur Pseudonymisierung bspw. European Union Agency For Network and Information Security (im Folgenden „ENISA"), Recommendations on shaping technology according to GDPR provisions, abrufbar unter https://www.enisa.europa.eu/publications/recommendations-on-shaping-tecnology-according-to-gdpr-provisions (Abruf: 16.9.2019), sowie *Schwartmann/Weiß*, Anforderungen an den datenschutzkonformen Einsatz von Pseudonymisierungslösungen, abrufbar unter https://www.gdd.de/downloads/whitepaper-zur-pseudonymisierung (Abruf: 16.9.2019).

9 Zu den Rechenschaftspflichten und Dokumentation, vgl. *Schild*, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Aufl. 2019, II. Kap. 5 B. II., Rn. 19.

auch Einfluss finden. So wird derzeit ein neuer ISO-Standard (ISO/AWI 31700) zum Thema „Konsumentenschutz: Privacy by Design für Konsumentenwaren und -dienstleistungen“[10] erarbeitet, der vor allem für Anbieter digital vernetzter Konsumprodukte – wie bspw. Smart-Home Geräte, Wearables, Mobile Apps und Online Services – hoch relevant sein wird.[11]

Für die Softwareentwicklung bedeuten die datenschutzrechtlichen Grundsätze des Art. 25 DSGVO letztendlich, dass jeder Softwarehersteller die Verantwortung dafür trägt, dass für jeden Anwender effektiver Datenschutz gewährleistet wird.[12] Dies ergibt sich im Übrigen auch aus dem Erwägungsgrund zur DSGVO Nr. 78 S. 4. Danach hat der Hersteller den Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen […] zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik [sicher zustellen], dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen.[13] Es sollte hierbei selbsterklärend sein, dass Softwareprodukte keinen Mehrwert für Verantwortliche (die späteren Abnehmer) bieten, wenn datenschutzrechtliche Vorgaben nicht eingehalten werden.[14]

Außerdem liegt im Zweifel auch ein Sachmangel vor, sollte das Produkt nicht datenschutzkonform sein – insbesondere müssen die aufgezeigten Anforderungen des Art. 25 DSGVO eingehalten werden,[15] da die objektive Gebrauchstauglichkeit von Software in der Regel nur dann gegeben ist, wenn gesetzliche Vorgaben eingehalten sind.[16]

2. Datenschutz in der Arbeitsorganisation

Die rechtlichen Rahmenbedingungen betreffen jedoch nicht nur die Softwareentwicklung, sondern auch die Arbeitsorganisation agiler Projekte. Insbesondere ist hier auf die Einhaltung des Beschäftigtendatenschutzes zu achten, da oftmals auch Beschäftigtendaten im Rahmen agiler Projekte offengelegt werden.[17] Hier kommen die folgenden Rechtsgrundlagen für die jeweilige Datenverarbeitung in Betracht:

– § 26 Abs. 1 S. 1 BDSG
– § 26 Abs. 4 BDSG, Art. 88 Abs. 4 DSGVO, i.V.m. einer Betriebsvereinbarung
– Einwilligung nach Art. 6 Abs. 1 lit. a) DSGVO i.V.m. § 26 Abs. 2 BDSG

Falls die Datenverarbeitung auf eine Betriebsvereinbarung nach § 26 Abs. 4 BDSG, Art. 88 Abs. 4 DSGVO gestützt wird, sind gerade ältere Betriebsvereinbarungen (insbesondere Betriebsvereinbarungen, die vor dem Inkrafttreten der DSGVO vereinbart wurden) daraufhin zu untersuchen, ob diese noch den datenschutzrechtlichen Anforderungen entsprechen. Darüber hinaus gilt, dass datenschutzrechtlich notwendige Informationen nach Art. 13, 14 DSGVO über einen geeigneten betriebsinternen Kommunikationsweg an den betroffenen Mitarbeiter herangetragen werden müssen.[18]

Exkurs: Weitere arbeitsrechtliche Anforderungen im Rahmen der agilen Organisation.

Zudem können im Anwendungsbereich des Betriebsverfassungsgesetztes (BetrVG) auch Informations-, Beratungs- oder Mitbestimmungsrechte des Betriebsrates von Relevanz sein, die keine datenschutzrechtliche Relevanz entfalten, aber im Rahmen von agilen Methoden aufkommen können.[19] So sind bei der Implementierung von agilen Methoden Unterrichtungs- und Beratungsrechte des Betriebsrates nach § 90 Abs. 1 BetrVG zu berücksichtigen.[20] Es sollte insbesondere darauf geachtet werden, dass die Unterrichtung „rechtzeitig“ erfolgt. Als verspätet könnte die Unterrichtung angesehen werden, wenn dem Betriebsrat ein vollständiges – mithin finales – Konzept zur Umsetzung agiler Methoden lediglich zur Zustimmung vorgelegt wird.[21]

Darüber hinaus ist die Mitbestimmung in wirtschaftlichen Angelegenheiten nach §§ 111 ff. BetrVG zu berücksichtigen, da die mit der Einführung von agilen Arbeitsmethoden einhergehenden Veränderungen die Voraussetzungen der § 111 S. 3 Nr. 4, 5 BetrVG erfüllen können. Eine Betriebsänderung nach § 111 S. 3 Nr. 1–5 BetrVG liegt jedoch nur dann vor, wenn die Änderung „einschneidende Auswirkungen auf den Betriebsablauf, die Arbeitsweise oder die Arbeitsbedingungen der Arbeitnehmer hat. Die Änderung muss in ihrer Gesamtschau von erheblicher Bedeutung für den gesamten Betriebsablauf sein.“[22] Eine Sachverhaltsprüfung im Einzelfall ist diesbezüglich unerlässlich.

Des Weiteren kann je nach Einzelfall auch die Mitbestimmung in sozialen Angelegenheiten nach § 87 BetrVG, die Beteiligung bei Personalplanung und beruflicher Bildung, §§ 92 ff., 96 ff. BetrVG sowie die Mitbestimmung in personellen Angelegenheiten nach § 99 BetrVG relevant sein.[23]

II. Umsetzungsvorschläge datenschutzrechtlicher Vorgaben im Rahmen agiler Projekte

Im Folgenden wird sowohl der Umgang mit datenschutzrechtlichen Anforderungen an die Entwicklung bzw. das zu entwickelnde Produkt als auch an die Arbeitsorganisation aufgezeigt und mögliche Strategien erläutert.

1. Strategien zum Umgang mit datenschutzrechtlichen Anforderungen an die Entwicklung bzw. das zu entwickelnde Produkt

Es existieren verschiedene Ansätze, die zur Umsetzung der vorgenannten allgemein gehaltenen rechtlichen Anforderungen (vgl. Abschnitt I.) herangezogen werden können. Beispielhaft sei an dieser Stelle auf die Ausführungen der ENISA,[24] die „Six protection goals for privacy engineering“,[25] sowie die LINDDUN-[26] und PRIPARE-[27]Ansätze sowie die Guidelines des Europäischen Datenschutzbe-

10 Vgl. https://www.iso.org/committee/6935430.html (Abruf: 16.9.2019).
11 Vgl. https://www.iso.org/news/ref2291.html (Abruf: 16.9.2019).
12 European Data Protection Supervisor (im Folgenden: „EDPS“), Preliminary Opinion on privacy by design, Opinion 5/2018, 31.5.2018, abrufbar unter https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf (Abruf: 16.9.2019), S. 15.
13 VO (EU) 2016/679, Erwägungsgrund Nr. 78, S. 4.
14 *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 25 DSGVO, Rn. 21.
15 *Mantz*, in: Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 25 DSGVO, Rn. 80.
16 Vgl. hierzu bereits OLG Hamm, 14.11.1994 – 31 U 105/94, BB 1995, 2, NJW-RR 1995, 941.
17 Vgl. die Ausführungen zum Kanban-Board unter Ziff. II. 2. b).
18 *Reiserer/Christ/Heinz*, DStR 2018, 1501, 1506.
19 Nicht weiter behandelt werden die arbeitsrechtlichen Probleme in Bezug auf Scheinselbstständigkeit und Arbeitnehmerüberlassung. S. hierzu vertiefend *Kühn/Wulff*; CR 2018, 417–425.
20 *Günther/Böglmüller*, NZA 2019, 417, 420 f.
21 Vgl. hierzu *Schulze/Volk*, ArbR 2019, 404, 405.
22 BAG, 18.3.2008 – 1 ABR 77/06, NZA 2008, 957, 959, BB-Entscheidungsreport *Kappenhagen*, BB 2009, 1646.
23 Vgl. bspw. *Hoffmann-Remy*, DB 2018, 2757, 2757 f.
24 Vgl. ENISA, Privacy and Data Protection by Design – from policy to engineering, abrufbar unter https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design (Abruf: 16.9.2019), S. 18 ff.
25 Vgl. *Hansen/Jensen/Rost*, Protection Goals for Privacy Engineering, 2015 IEEE CS Security and Privacy Workshops, abrufbar unter https://ieeexplore.ieee.org/document/7163220 (Abruf: 16.9.2019).
26 Vgl. https://distrinet.cs.kuleuven.be/software/linddun/ (Abruf: 16.9.2019).
27 PRIPARE, Handbook – Privacy and Security by Design Methodology, abrufbar unter http://pripareproject.eu/wp-content/uploads/2013/11/PRIPARE-Methodology-Handbook-Final-Feb-24-2016.pdf (Abruf: 16.9.2019).

auftragten[28] verwiesen, welche hier in Teilen und zwar mit Blick auf die Scrum-Methode aufgegriffen werden.

Im Rahmen der klassischen Softwareentwicklung (sog. „Wasserfallmethode“[29]) kann recht klar identifiziert werden, wann eine datenschutzrechtliche Ausgestaltung bzw. Beratung erfolgen kann. Bereits im Rahmen der Planungs- und Konzeptionsphase wird ein vollständiger Plan (Lastenheft/Pflichtenheft[30]) erarbeitet, der bspw. dem Datenschutzbeauftragten/externen juristischen Berater zur Prüfung vorgelegt werden kann.[31] Mit der Realisierung wird erst begonnen, wenn diese Phase erfolgt ist.[32]

Bei agiler Entwicklung gibt es einen solchen festen Zeitpunkt nicht. Vergleichbar festgelegte Pläne sind der agilen Methode fremd und widersprechen dem Grundkonzept der iterativen Vorgehensweise der Scrum-Methode.[33] Daher kann eine datenschutzrechtliche Bewertung auf den ersten Blick erst am Ende erfolgen, wenn das Produkt fertig entwickelt ist. Sollten dann aber grundlegende Änderungen notwendig sein, wird dies nicht nur für das geplante finanzielle Budget, sondern auch für den Zeitplan zur Belastungsprobe. Daher sollten datenschutzrechtliche Vorgaben auch im Rahmen der Scrum-Methode möglichst frühzeitig und kontinuierlich berücksichtigt werden, da es sich andernfalls mit fortschreitendem Projektverlauf als zunehmend herausfordernd gestalten wird, datenschutzkonforme Produkte zu entwickeln.[34] In der Praxis ist die Versuchung oftmals groß, lediglich nachträglich minimale Anpassungen zur Risikominimierung vorzunehmen.[35] Um einen solchen „workaround“ zu vermeiden, sollten zwingendermaßen die oben aufgezeigten datenschutzrechtlichen Anforderungen auch oder gerade in dem iterativen Verfahren implementiert werden. Dies kann über das Product Backlog, die User Stories, die Sprints und die Sprint Reviews[36] erfolgen.

a) Product Backlog

Das Product Backlog stellt eine Liste mit Anforderungen an das jeweils zu entwickelnde Produkt dar.[37] Es ließe sich daher (vergleichbar zum Wasserfallmodell) bereits vor Entwicklungsbeginn zusammenfassen, welche datenschutzrechtlichen Anforderungen an das Produkt gestellt werden müssen. Hierbei besteht jedoch die Gefahr, dass diese zu allgemein gehalten wären, um zielführend zu sein, oder aber zu eng gefasst, sodass sie irrelevant sein könnten.[38]

Dennoch sollten die ebenfalls allgemein gehaltenen Datenschutzziele des Art. 5 DSGVO im Product Backlog festgehalten werden. Um dem Entwicklungsteam die Handhabung der Grundsätze zu erleichtern, könnte eine solche Liste visuell so festgehalten werden, dass sie bei jeder Designentscheidung als Orientierungshilfe herangezogen werden kann.[39] Von Vorteil ist es hierbei, dass das Product Backlog und die dort formulierten Anforderungen kontinuierlich vervollständigt werden können.[40] Daher sollte die Möglichkeit genutzt werden, im Laufe der agilen Produktentwicklung auch die im Product Backlog festgehaltenen datenschutzrechtlichen Anforderungen anzupassen, je genauer die Vorstellung von dem zu erstellenden Produkt selbst wird.

b) Epics/User Stories

Auch durch die Festlegung datenschutzrechtlicher Epics/User Stories kann ein Beitrag zu einer datenschutzkonformen Produktentwicklung geleistet werden. User Stories stellen Anforderungsprofile des Endnutzers an das Produkt dar, während Epics ein Bündel von User Stories unter einer Zielvorgabe zusammenfasst.[41] Über das sog. „privacy-tagging“ können Datenschutzanforderungen auch über User Stories und Epics in die agile Entwicklung eingebunden werden.[42] Hierbei werden datenschutzrechtlich geprägte Epics (bspw. „Es ist ein besonderer Schutz für Kinder zu gewährleisten“) und User Stories (bspw. „Als ein Kind ist es wichtig auf kindesgerechte Informationen zugreifen zu können, sodass Kinder die Risiken begreifen können und Schutzmaßnahmen etabliert sind, die den Schutz ihrer Daten innerhalb des Systems gewährleisten.“) erstellt.[43] Die Epics und User Stories werden anschließend mit einem „Tag“ versehen, der die Vorgaben der DSGVO enthält.[44] Wenn nun diesem „Tag“ eine Aufgabe („Task“) in der Projekterfassungssoftware zugewiesen wird, kann erreicht werden, dass die Einhaltung datenschutzrechtlicher Vorgaben als Aufgabenerledigung erfasst wird.[45] Damit ermöglicht diese Vorgehensweise es dem Verantwortlichen, zu dokumentieren, welche datenschutzrechtlichen Vorgaben im Rahmen der Entwicklung auf welche Weise umgesetzt wurden.

c) Sprint

Die Sprints stellen variable Zeitfenster von meist einem Monat oder weniger dar, in denen ein fertiges Produktinkrement (das sogenannte „shipable product“) erstellt werden soll.[46] Bereits hier sollte berücksichtigt werden, dass immer auch ein grundsätzlich datenschutzkonformes Produkt aus den einzelnen Sprints hervorgehen sollte.

Während des ersten Sprints (dem „Sprint Zero“) sollte daher ein sogenanntes Datenflussdiagramm[47] aufgesetzt werden, das während des gesamten agilen Projekts den aktuellen Entwicklungen angepasst werden sollte.[48] Durch dieses Datenflussdiagramm sollten folgende Fragen beantwortet werden:

- Aus welcher Quelle stammen die personenbezogenen Daten, an welchem Ort werden sie gespeichert?
- Welche Prozesse sowie interne/externe Stellen greifen auf die Daten zu und ist der Zugriff notwendig?
- Für wie lange werden die Daten aufbewahrt und wie wird die Löschung umgesetzt (Löschung, Anonymisierung etc.)?

28 EDPS, Guidelines on the protection of personal data in IT governance and IT management, abrufbar unter https://edps.europa.eu/sites/edp/files/publication/it_governance_management_en.pdf (Abruf: 16.9.2019).
29 Vgl. hierzu bspw. *Conrad/Witzel*, in: Auer-Reinsdorff/Conrad, Hb. IT- und Datenschutzrecht, 2. Aufl. 2016, § 18, Rn. 132.
30 Vgl. zur Begriffsbestimmung bspw. *Redeker*, in: Redeker, IT-Recht, 6. Aufl. 2017, B., Rn. 302 ff.
31 *Koglin*, in: Bussche v. d./Voigt, Konzerndatenschutz, 2. Aufl. 2019, Kap. 5., Rn. 48.
32 *Conrad/Witzel*, in: Auer-Reinsdorff/Conrad, Hb. IT- und Datenschutzrecht, 2. Aufl. 2016, § 18, Rn. 132–138.
33 Vgl. umfassend zur Scrum Methodik *Schwaber/Sutherland*, The Scrum Guide, abrufbar unter https://www.scrumguides.org/scrum-guide.html (Abruf 16.9.2019).
34 *Viitaniemi*, Privacy by design in agile software development, abrufbar unter https://dspace.cc.tut.fi/dpub/bitstream/handle/123456789/25321/Viitaniemi.pdf (Abruf: 16.9.2019), S. 13.
35 Vgl. zur Problematik der Durchführung einer Datenschutz-Folgenabschätzung in agilen Prozessen: *Koglin*, in: Koreng/Lachenmann, Formularhandbuch Datenschutzrecht, 2. Aufl. 2018, A. III. 7.
36 Zu den Begrifflichkeiten im Einzelnen vgl. bspw. *Schwaber/Sutherland* (Fn. 33).
37 *Schwaber/Sutherland* (Fn. 33).
38 *Viitaniemi* (Fn. 34), S. 14.
39 *Viitaniemi* (Fn. 34), S. 33; *Schwaber/Sutherland* (Fn. 33).
40 *Schwaber/Sutherland* (Fn. 33).
41 Vgl. bspw. https://www.atlassian.com/agile/project-management/epics-stories-themes (Abruf: 10.9.2019).
42 Vgl. *Miri/Foomany/Mohammed*, Complying with GDPR: An Agile Case Study, ISACA Journal Volume 2, 2018.
43 *Miri/Foomany/Mohammed* (Fn. 42).
44 *Miri/Foomany/Mohammed* (Fn. 42).
45 *Miri/Foomany/Mohammed* (Fn. 42).
46 *Schwaber/Sutherland* (Fn. 33).
47 Vgl. die hierzu gehörige LINDDUN-Methode, abrufbar unter https://distrinet.cs.kuleuven.be/software/linddun/ (Abruf: 16.9.2019).
48 *Viitaniemi* (Fn. 34), S. 34.

Wenn das Datenflussdiagramm zusammengestellt ist, soll ein möglichst ganzheitlicher Überblick über das Produkt-Design sowie sämtlicher Datenströme vorliegen. Zur besseren Übersichtlichkeit sollte die Anzahl an Diagrammen der Projektgröße angepasst werden.[49] Anderenfalls läuft das Entwicklungsteam Gefahr, Datenströme zu übersehen.

Während des iterativen Prozesses muss die Pflege des Datenflussdiagramms möglichst reibungslos in die Arbeitsweise des Entwicklerteams integriert werden. Deshalb sollte das gesamte Entwicklerteam diese Diagramme anpassen können, sodass bspw. neu auftretende Datenschutzanforderungen dokumentiert werden können.[50] Sollten Probleme im Umgang mit den Diagrammen auftreten, können diese im Rahmen der Scrum Retrospektive beseitigt werden.[51]

Durch die gewissenhafte Pflege von Datenflussdiagrammen wird zusätzlich ein wesentlicher Beitrag zur Datenminimierung geleistet: Zunächst kann das Entwicklungsteam (und damit ggf. auch der datenschutzrechtliche Berater) erkennen, wie viele personenbezogenen Daten in dem System verarbeitet werden. Hieran sollte sich eine Prüfung anschließen, ob sämtliche personenbezogene Daten auch notwendigerweise verarbeitet werden müssen.[52] Redundante Verarbeitungsvorgänge können und müssen dann im Designprozess eliminiert werden.

d) Sprint Review

Im Sprint Review kann schließlich überprüft werden, ob die vorab identifizierten datenschutzrelevanten Punkte eingehalten wurden.[53] Unvollendete Aufgaben müssen im Rahmen des Sprint Reviews auf einen Folgesprint übertragen werden.

Folgende Fragestellungen können sich bei der Durchführung des Sprint Reviews – im Rahmen der Überprüfung des Produktinkrements – als nützlich erweisen:[54]

– Verarbeitet das Inkrement personenbezogene Daten?
– Erfolgt eine Verknüpfung von Daten mit personenbezogenen Daten durch das Inkrement?
– Bringt das Inkrement personenbezogene Daten in ein Modul ein, das zuvor keine personenbezogenen Daten verarbeitet hat?
– Hat das Inkrement Auswirkungen auf die im Product Backlog festgelegten Datenschutzziele?

Damit keine datenschutzrechtlich relevanten Informationen verloren gehen, sollten aufgrund dieser Antworten zur besseren Übersichtlichkeit ebenfalls eine Anpassung des Datenflussdiagramms durchgeführt werden.

2. Strategien zum Umgang mit datenschutzrechtlichen Anforderungen an die Arbeitsorganisation

Auch im Rahmen der Methodik selbst bzw. der Arbeitsorganisation ergeben sich wie bereits aufgezeigt datenschutzrechtliche Herausforderungen. Hierbei werden neben den eingesetzten IT-Tools sog. Kanban-Boards relevant.

a) IT-Tool Einsatz

Zusätzliche Herausforderungen ergeben sich dadurch, dass die Auswahl an Softwareentwicklungs-Tools durch datenschutzrechtliche Vorgaben eingeschränkt sein kann. Hierbei geht es weniger um die datenschutzrechtliche Tauglichkeit des zu entwickelnden Produktes, sondern neben den Beschäftigtendaten, die in enthalten sein können, vorrangig um die Verarbeitung von personenbezogenen (Test-)Daten, die der Hersteller vom Kunden erhalten hat. Daher sollte vor Einsatz derartiger Tools überprüft werden, ob der jeweilige Softwareeinsatz (bspw. Projektmanagement-Tool „Jira“[55] oder Dokumentations- und Kommunikations-Tools „Confluence“[56]) datenschutzrechtliche Relevanz hat und zulässig ist. Hierbei kommt es neben der vertraglichen Ausgestaltung mit dem Softwareanbieter aber auch auf die Anzahl, die Art und die konkrete Verarbeitung der personenbezogenen Daten an, so dass hier keine abstrakte Betrachtung erfolgen kann. Spannend ist in jedem Fall, dass in der Praxis oftmals betretenes Schweigen herrscht, wenn man sich im Rahmen von agilen Meet-Ups danach erkundigt, ob und wie der Datenschutz in den agilen IT-Tools umgesetzt wird, da oftmals das Bewusstsein für die Relevanz fehlt. Es lohnt daher immer, auch die eingesetzten IT-Tools zu betrachten und den Entwickler im Rahmen einer Auftragsentwicklung nach den eingesetzten Tools zu befragen, sofern denn personenbezogene Daten im Rahmen der Entwicklung zum Einsatz kommen sollen.

b) Kanban-Board

Kanban wird nach Scrum als zweithäufigste agile Projektmanagement-Methode eingesetzt,[57] und wird oft zur Organisation von Teams oder Prozessen eingesetzt, sodass sich auch hier ein Blick auf mögliche rechtliche Hürden lohnt. Bei den zum Einsatz kommenden Kanban-Boards wird auf Karten jeweils eine Arbeitsaufgabe festgehalten und diese auf dem Board in der zutreffenden Spalte (bspw. „Planung“, „Bearbeitung“, „Erledigt“) platziert, damit der aktuelle Arbeitsfortschritt visuell erkennbar und planbar wird.[58] Hierbei ist zu beachten, dass diese Karten Informationen beinhalten, die eine umfassende Visualisierung des aktuellen Workflows von IT-Entwicklungsteams bis hin zu Unternehmen ermöglichen.[59]

Der Einsatz von Kanban-Boards wirft vor allem Fragen aus dem Arbeitnehmerdatenschutz auf, denn wenn eine Dokumentation des aktuellen Workflows visuell festgehalten wird, liegt der Gedanke nahe, dass Arbeitgeber diese Ergebnisse für Mitarbeiterkontrollen verwenden. Hierbei gilt, dass Arbeitgeber grundsätzlich ein jederzeitiges uneingeschränktes Einsichtsrecht in dienstliche Unterlagen haben,[60] außer die tatsächliche Einsichtsmaßnahme des Arbeitsgebers betrifft personenbezogene Daten.[61] Personenbezogene Daten nach Art. 4 Nr. 1 DSGVO liegen dann vor, wenn bspw. jedem Mitarbeiter eine Farbe für Kanban-Karten zugeteilt wird oder der jeweilige Name des Mitarbeiters als Bearbeiter auf Kanban-Karten notiert wird. Gleiches kann gelten, wenn der Arbeitgeber das Kanban-Board als Grundlage für Rückfragen über „persönliche und sachliche Verhältnisse“[62] der Arbeitnehmer verwendet. Eine Rechtfertigung von Kontrollmaßnah-

49 *Viitaniemi* (Fn. 34), S. 35.
50 *Viitaniemi* (Fn. 34), S. 37 f.
51 *Sutherland/Schwaber*, The Scrum Guide: The Definitive Guide to Scrum: The Rules of the Game, abrufbar unter http://www.Scrum-guides.org/docs/Scrumguide/v1/Scrum-Guide-US.pdf#zoom=100 (Abruf: 16.9.2019).
52 *Viitaniemi* (Fn. 34), S. 41.
53 *Viitaniemi* (Fn. 34), S. 40.
54 Hierzu vgl. *Viitaniemi* (Fn. 34), S. 39.
55 Vgl. https://www.atlassian.com/software/jira (Abruf: 16.9.2019).
56 Vgl. https://www.atlassian.com/de/software/confluence (Abruf: 16.9.2019).
57 Vgl. bitkom, https://www.bitkom-research.de/de/pressemitteilung/scrum-koenig-unter-den-agilen-methoden (Abruf: 23.9.2019).
58 *Degradis/Karu*, Using Kanban for IT Operations, abrufbar unter https://resources.leankit.com/guides/using-kanban-for-it-operations (Abruf: 16.9.2019).
59 *Degradis/Karu* (Fn. 58).
60 *Wessing*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, 3. Aufl. 2016, § 46, Rn. 30.
61 *Wessing*, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, 3. Aufl. 2016, § 46, Rn. 31; zum weiteren Anwendungsbereich des § 26 Abs. 7 BDSG verglichen zu Art. 2 Abs. 2 DSGVO vgl. bspw. *Maschmann*, NZA-BL 2018, 115, 115.
62 Hierzu vgl. *Maschmann*, NZA-BL 2018, 115, 115.

men käme dann über § 26 Abs. 1 S. 1 BDSG infrage, wenn die Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses erfolgt und hierfür auch erforderlich ist. Die hierfür notwendige Erforderlichkeit wird aber nur dann vorliegen, wenn der Arbeitgeber die Daten vernünftigerweise benötigt, so bspw. im Rahmen der Ausübung der Weisungs- und Kontrollrechte.[63] Im Regelfall sollte eine Überprüfung des Einsatzes von Personalressourcen und der Nachjustierung – wenn die Bearbeitung einzelner Tasks zu einem Arbeitsrückstau führt – durch den Arbeitgeber beabsichtigt sein. Eine derartige Überprüfung weist nur eine geringe Eingriffsintensität vor, sodass die schutzwürdigen Interessen des Arbeitgebers an der Ausübung der Weisungs- und Kontrollrechte denen des Arbeitnehmers überwiegen.

Alternativ kann an den Abschluss einer Betriebsvereinbarung nach § 26 Abs. 4 BDSG gedacht werden, um Datenverarbeitungen beim Einsatz von Kanban zu regeln. Denkbar ist auch ein Rückgriff auf die Einwilligungslösung nach Art. 6 Abs. 1 lit. a) DSGVO i.V.m. § 26 Abs. 2 BDSG der hier aber als Ultima Ratio nicht opportun ist.

3. „Agile Lawyer"

Schließlich bleibt die Frage, wie bzw. durch wen das datenschutzrechtliche Wissen und die Anfreundungen an die Entwicklung in das Projekt eingebracht werden. Hier kann die Eingliederung (externer) Anwälte in iterative Verfahren Mehrwerte bieten. Der Erfolg dieses Ansatzes hängt jedoch wesentlich von den Vorkenntnissen des jeweiligen Anwalts ab. Idealerweise verfügt der Rechtsberater über Kenntnisse bzgl. agiler Verfahren, der generellen Rollenverteilung der Scrumbeteiligten sowie die eigene (neue) Rolle im Scrum-Verfahren.

Des Weiteren hängt der Erfolg dieser engen Begleitung durch einen „agile Lawyer" von der tatsächlichen Einbindung in das agile Projekt ab. Vorteil dieses Ansatzes sollte es sein, dass möglichst frühzeitig und proaktiv eine datenschutzkonforme Projektentwicklung gewährleistet werden kann.[64] Die Einschaltung einer zusätzlichen – nicht im agilen Manifest vorgesehenen – Rolle ruft jedoch die Gefahr der nicht gewollten Beeinflussung des Prozesses[65] bis hin zur Prozessverlangsamung hervor.

Um dem entgegenzuwirken, sollte der Einsatz von Rechtsberatern konzeptionell durchdacht sein. Dabei kann der rechtliche Input des „agile Lawyer" auf zwei Wegen in das Produkt einfließen:

aa) Der „agile Lawyer" schreibt selbst Teile des Product Backlogs/der User Stories. Hierbei stößt man jedoch wieder auf das Problem, dass die „Anweisungen" entweder zu grob gefasst sind und deshalb nicht dazu beitragen, dass ein datenschutzrechtlicher Mehrwert geschaffen wird. Andererseits könnten die Angaben zu detailliert sein und dadurch das Entwicklungsteam zu sehr eingeschränkt werden.

bb) Es erfolgt eine unmittelbare juristische Beratung des Entwicklungsteams/des Product Owners. Diese haben dann dafür Sorge zu tragen, dass der Input in dem jeweiligen Sprint Backlog Einfluss findet.

Gerade der zuletzt genannte Ansatz bietet dann einen Mehrwert, wenn möglichst frühzeitig ein mit dem agilen Mindset vertrauter Rechtsberater eingeschaltet wird. Wenn die zuvor besprochenen Zusammenhänge bekannt sind, sollte der „agile Lawyer" nicht als Fremdkörper wahrgenommen werden. Stattdessen könnte er das iterative Verfahren beschleunigen, wenn bspw. Unklarheiten zu einem erstellten Datenflussdiagramm vorliegen. Von Mehrwert ist dies allemal, wenn hierdurch proaktiv verhindert wird, dass sich Entwicklerteams in datenschutzrechtlich schwer zu lösende Lagen begeben.[66] Daher verwundert es nicht, dass dieser Ansatz im Gespräch mit Scrum Mastern und Scrum Coaches, Product Ownern usw. auf regen Zuspruch stößt.

III. Fazit

Werden die zuvor beschriebenen proaktiven Lösungsvorschläge in die agile Methode integriert, sollte die datenschutzkonforme Produktentwicklung und Arbeitsorganisation effizienter gelingen. Wie zuvor gezeigt, sollte ein betriebswirtschaftlicher Anreiz darin liegen, einen möglichst großen Kundenmehrwert durch datenschutzkonforme Produkte zu schaffen und diesen „added-value" als eigenen Produktvorteil am Markt zu bewerben. Es existiert bereits die allgemeine Erwartungshaltung an Entwickler, dass die unter Abschnitt I. beschriebenen Anforderungen an Privacy by Design und Privacy by Default eingehalten werden. Wenn Entwickler bspw. die erwähnten nachgelagerten datenschutzrechtlichen Dokumentationspflichten des späteren Verantwortlichen erleichtern, sollte es betriebswirtschaftlich möglich sein, die zusätzlichen Kosten für ein datenschutzkonformes agiles Produkt in den Gesamtpreis einfließen zu lassen. Schlussendlich sollte nicht vergessen werden, dass nur ein anwenderfreundliches und zugleich auch datenschutzkonformes Produkt auch Aussicht auf wirtschaftlichen Erfolg hat. Hierin kann ein nicht zu vernachlässigender Wettbewerbsvorteil liegen.

Philipp M. Kühn, RA, ist Senior Associate in der Praxisgruppe IT/IP/Datenschutzrecht von Ebner Stolz am Standort Köln. Er berät bundesweit Konzerne, mittelständische Firmen sowie Start-ups zu allen rechtlichen Fragen des Datenschutz- und IT-Rechts. Dies umfasst insbesondere alle Fragen rund um den Einsatz agiler Methoden, IoT und Digital Health sowie Transaktionen und Sourcingprozesse. Er spricht und veröffentlicht regelmäßig zu (agilen) juristischen Themen und engagiert sich beim Scrumtisch Köln und Bonn.

Neil C. Weaver, LL.B., RA, ist Associate in der Praxisgruppe IT/IP/Datenschutzrecht von Ebner Stolz am Standort Köln. Er berät zu allen Fragen des Informationstechnologie- und Datenschutzrechts, mit einem besonderen Fokus auf die IT-Vertragsgestaltung.

63 *Zöll*, in: Taeger/Gabel, DSGVO BDSG, 3. Aufl. 2019, § 26 BDSG, Rn. 38.
64 *Koglin*, in: Koreng/Lachenmann, Formularhandbuch Datenschutzrecht, 2. Aufl. 2018, A. III. 7.; Vgl. zum „agilen Patentanwalt", *Koch*, BB 2017, 387, 389.
65 *Koch*, BB 2017, 387, 389.
66 *Koch*, BB 2017, 387, 389.