Ralf Kneuper, Sven Jacobs

Softwaretest mit Originaldaten

Eine Analyse aus Sicht des Datenschutzes

Der Wunsch nach einer Nutzung von Originaldaten für den Softwaretest führt in bestimmten Konstellationen zu einem Konflikt zwischen der Zweckbeschränkung von personenbezogenen Daten einerseits und der Forderung nach Qualitätssicherung der Systeme zur Verarbeitung dieser Daten andererseits. Der Beitrag begründet, warum die Nutzung von Originaldaten nach Möglichkeit vermieden werden sollte, bei Bedarf aber unter eng begrenzten Rahmenbedingungen rechtlich möglich ist.

1 Hintergrund

1.1 Problemstellung

Ein Konfliktpunkt in der Softwareentwicklung in Bezug auf den Datenschutz ist die Nutzung von personenbezogenen Originaldaten (Echtdaten) für den Softwaretest.[1] Die Herausforderung dabei besteht darin, dass die Originaldaten üblicherweise für die relevanten Geschäftsprozesse, aber nicht für den Test erhoben wurden, und auch die Information der Betroffenen oder ggf. deren Einwilligung die Nutzung der Daten für den Test von Software normalerweise nicht ausdrücklich einschließen.

Bei einem gewünschten Softwaretest mit Originaldaten sind daher folgende Fragen zu klären:

- Ist die Nutzung personenbezogener Daten für den Softwaretest erlaubt? Auf welcher Rechtsgrundlage und unter welchen Rahmenbedingungen?
- Inwieweit müssen die Betroffenen über die Nutzung ihrer Daten für den Softwaretest informiert werden?

Diese Fragen sollten in diesem Beitrag analysiert und beantwortet werden.

Zusätzlich handelt es sich bei der Softwareentwicklung oft um eine Form der Auftragsverarbeitung, sodass die dafür üblichen Anforderungen, insbesondere der Abschluss einer entsprechenden Vereinbarung zwischen dem Verantwortlichen und der Softwareentwicklungsorganisation, erfüllt werden müssen. Hier gibt es aber keine Besonderheiten in Bezug auf den Softwaretest, so dass auf diesen Aspekt nicht weiter eingegangen werden soll.

1.2 Warum Testen mit Originaldaten?

Bevor wir die genannten Fragen beantworten können, stellt sich zuerst einmal die Frage nach dem Zweck des Tests mit Originaldaten. Für die folgende Diskussion gehen wir von einem typischen einfachen Testablauf mit den Stufen Modultest (Unittest), Integrationstest und Systemtest aus.

Für die ersten beiden Teststufen ist ein Test auf Basis von Originaldaten nicht geeignet, da hier normalerweise keine Soll-Ergebnisse für einen Soll-Ist-Vergleich vorliegen, der aber einen Kernbestandteil der meisten Testformen bildet. Erst wenn die einzelnen Module (Modultest), deren Zusammenwirken (Integrationstest) sowie das gesamte zu entwickelnde System (erster Teil des Systemtests) gründlich mit künstlichen Testdaten getestet wurden und kaum noch Fehler aufweisen, kommt schon aus Sicht der Testmethodik ein Test mit Originaldaten in Frage. Bei diesem letzten Teil des Systemtests geht es um die Prüfung, ob alle real auftretenden Sonderfälle auch von der entwickelten Software berücksichtigt werden. Dabei wird in der Praxis meist nur geprüft, dass die Software die Daten ohne Fehlermeldungen durchläuft, da aufgrund fehlender überprüfter Soll-Ergebnisse eine Prüfung der funktionalen Korrektheit der Ergebnisse meist nicht möglich ist.

Gemäß dem Grundsatz der Datenminimierung sollte auch dieser Teil des Systemtestes nach Möglichkeit mit anonymisierten Daten durchgeführt werden, aber je nach Rahmenbedingungen und Art des Systems reicht ein solcher Test nicht immer aus. Ein Bedarf an einem Test mit Originaldaten besteht beispielsweise bei einer Datenmigration in ein neues Kernsystem einer Versiche-

1 Siehe beispielsweise den Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten 2006/07 [1] oder das Datenschutz-Wiki [2].

Prof. Dr. Ralf Kneuper

ist Professor für Wirtschaftsinformatik und Studiengangleiter Informatik an der IUBH Internationale Hochschule in Bad Reichenhall.

E-Mail: r.kneuper@iubh-fernstudium.de

Sven Jacobs

Corporate Counsel und Deputy Head Regulatory EMEAR sowie Lehrbeauftragter der Hector School des KIT Karlsruhe und der IUBH Internationale Hochschule – Fernstudium.

E-Mail: sv.jacobs@iubh-fernstudium.de

rung. Hier bestehen einerseits hohe Anforderungen an die Korrektheit bzw. die systematische Prüfung des neuen Systems, die ggf. sogar gegenüber der zuständigen Aufsichtsbehörde nachzuweisen ist, andererseits viele über Jahre entstandene Sonderfälle, die in der Entwicklung möglicherweise nicht alle bekannt sind.

Auch bei einer Entscheidung für eine Anonymisierung der Originaldaten ist zu berücksichtigen, dass durch die bei der Anonymisierung verursachte Veränderung der Daten möglicherweise der Testzweck nicht mehr erreicht wird, weil beispielsweise bestimmte Abhängigkeiten oder unerwartete Konstellationen in den anonymisierten Daten nicht mehr vorhanden sind.

Eine Pseudonymisierung der Daten ist in diesem Kontext dagegen nicht relevant, da die Möglichkeit einer späteren Zuordnung der Daten zur Person für den betrachteten Zweck des Testens keinen Nutzen bringt. Wenn ein Test mit pseudonymisierten Daten möglich ist, dann ist er ohne weitere Einschränkung auch mit anonymisierten Daten möglich, und daher sollte immer diese stärkere Schutzmaßnahme angewendet werden.

Daneben werden Originaldaten auch für die Analyse von Fehlermeldungen und den Test der Fehlerkorrektur genutzt, wenn ein Fehler sonst nicht nachzuvollziehen ist.

Ein weiterer Anwendungsbereich des Tests mit Originaldaten betrifft den Performanztest, hier wie üblich als Bestandteil des Systemtests betrachtet, bei dem es in erster Linie um die Geschwindigkeit geht, mit der eine große Menge von Daten bearbeitet wird. Hier ist es grundsätzlich möglich, aber ggf. sehr schwierig, eine angemessene Menge von Testdaten einschließlich der benötigten Sonderfälle künstlich zu erzeugen, sodass auch hier oft der Wunsch nach der Nutzung von Originaldaten für den Test besteht.

Bisher ging die Betrachtung davon aus, dass der Test in einer separaten Testumgebung durchgeführt wird und nicht in der Produktivumgebung. Dies ist normalerweise schon aus testfachlicher Sicht erforderlich, aber es gibt Ausnahmen, insbesondere beim Test von Fehlerkorrekturen, in denen das nicht sinnvoll möglich ist, so dass in Einzelfällen auch ein Test in der Produktivumgebung erforderlich sein kann.

1.3 Warum kein Testen mit Originaldaten?

Gegen das Testen mit Originaldaten spricht, dass im Allgemeinen wesentlich mehr Personen Zugriff auf Testsysteme haben als das bei Produktivsystemen der Fall ist. Auch werden die Testergebnisse oft weitergegeben, ohne dass geprüft wird, ob sie personenbezogene Daten enthalten [2]. Darüber hinaus wird durch eine solche Verarbeitung die Gefahr von Datenpannen vergrößert, da die Daten auf zusätzlichen und noch nicht abschließend entwickelten und daher fehleranfälligen Systemen eingesetzt werden. Das gilt insbesondere, wenn der Test nicht in einer separaten Testumgebung, sondern in der Produktivumgebung durchgeführt wird. Darüber hinaus ist zu berücksichtigen, dass Testdaten häufig nicht die gleiche Sorgfalt entgegengebracht wird wie das für personenbezogene Daten im Produktivbetrieb gefordert und üblich ist.

1.4 Grundlegende Voraussetzungen

Aufgrund der vorgenannten Risiken sowie des Grundsatzes der Datenminimierung sollte zwingend geprüft werden, ob (a) fiktive Testdaten generiert oder (b) die Originaldaten anonymisiert werden können. Die weitere Diskussion in diesem Beitrag geht davon aus, dass diese Prüfung stattgefunden hat mit dem Ergebnis, dass der Testzweck mit fiktiven Testdaten oder anonymisierten Originaldaten nicht oder nicht angemessen erreicht werden kann.

Darüber hinaus ist es wichtig, eine angemessene und dem Produktivbetrieb vergleichbare Sicherheit der Daten bei der Nutzung von Originaldaten für den Softwaretest sicherzustellen, denn für die geforderte Datensicherheit macht es keinen Unterschied, ob Daten zu Produktiv- oder zu Testzwecken verwendet werden. Beispielsweise muss der Zugriff auf die im Test verwendeten Originaldaten restriktiv gehandhabt werden und darf nur einer möglichst kleinen Gruppe von Testern und Entwicklern erlaubt werden. Nach Bedarf ist dies durch eine Datenschutz-Folgenabschätzung oder eine Abstimmung mit der jeweils zuständigen Datenschutzbehörde abzuklären.

2 Unterschiedliche Ausgangssituationen im Rahmen von Softwaretests

2.1 Beziehung zwischen ursprünglichem Zweck und Zweck des Tests

Für die Beantwortung der vorgenannten Ausgangsfragen müssen aus Sicht des Datenschutzes folgende Ausgangssituationen und Rahmenbedingungen unterschieden werden:

1. Die ursprüngliche Verarbeitung basiert auf einer Einwilligung als Rechtsgrundlage.
2. Die ursprüngliche Verarbeitung beruht nicht auf einer Einwilligung; der Test mit Originaldaten ist Bestandteil des ursprünglich definierten Zwecks.
3. Die ursprüngliche Verarbeitung beruht nicht auf einer Einwilligung; der Test mit Originaldaten ist vereinbar (kompatibel) mit dem ursprünglich definierten Zweck.
4. Die ursprüngliche Verarbeitung beruht nicht auf einer Einwilligung; der Test mit Originaldaten ist nicht vereinbar mit dem ursprünglich definierten Zweck.

Aus der Entscheidung, welcher dieser Fälle vorliegt, ergeben sich nach der DSGVO eine Reihe von sehr unterschiedlichen Konsequenzen für die betrachtete Problemstellung, die im Folgenden ab Abschnitt 3 analysiert werden. Zuerst ist aber eine genauere Unterscheidung erforderlich, wann welcher der genannten Fälle gegeben ist.

2.2 Ursprüngliche Verarbeitung auf Grundlage einer Einwilligung

Diese Fallgruppe ist separat zu betrachten, denn eine wesentliche Eigenschaft einer gültigen Einwilligung ist ihre Bestimmtheit, d. h. wenn Betroffene in eine bestimmte Verarbeitung einwilligen, dann sind diese Verarbeitung und ihr Zweck relativ restriktiv zu interpretieren. Daher ist dieser Fall bei der Definition einer kompatiblen Zweckänderung in Art. 6 Abs. 4 DSGVO ausdrücklich ausgeschlossen. Die Konsequenzen, die sich daraus ergeben, werden in Abschnitt 3 näher betrachtet.[2]

2 Genau genommen ist eine kompatible Zweckänderung auch für den Fall ausgeschlossen, dass die ursprüngliche Verarbeitung auf einer Rechtsvorschrift der Union oder der Mitgliedsstaaten beruht, die der nationalen Sicherheit oder ähnlichen Zwecken dient. Dieser Fall ist aber im Kontext des Softwaretests kaum relevant.

2.3 Test als Bestandteil des ursprünglichen Zwecks

Die für den Softwaretest herangezogenen personenbezogenen Daten werden üblicherweise für einen bestimmten Verarbeitungszweck erhoben, bei dem der Test nicht ausdrücklich enthalten ist. Auch dabei stellt sich aber die Frage, ob es sich bei der Nutzung der Daten für den Softwaretest in jedem Fall um eine Zweckänderung handelt: Unabhängig davon, ob die Verarbeitung auf einer Einwilligung (hier nicht betrachtet) oder einer anderen Rechtsgrundlage beruht, haben die Betroffenen ihre Daten ausdrücklich oder implizit für eine bestimmte Verarbeitung bereitgestellt, und um diese Verarbeitung durchführen zu können, benötigt der Verantwortliche angemessen entwickelte und getestete IT-Systeme.

Daraus lässt sich folgern, dass der Test mit Originaldaten in diesem Fall dem ursprünglich definierten Zweck der Verarbeitung dient, es sich also um keine Zweckänderung handelt. Für die sehr ähnliche Verarbeitung zur „Wahrnehmung von Aufsichts- und Kontrollbefugnissen" wurde in § 14 Abs. 3 BDSG a. F. explizit formuliert, dass es sich hierbei nicht um eine Zweckänderung handelt.

Voraussetzung dafür ist, dass das zu testende System wirklich dem Zweck der ursprünglichen Verarbeitung dient, es sich also um eine Weiterentwicklung, Fehlerkorrektur oder Migration auf eine neue technische Basis handelt und nicht um eine komplett neue Funktionalität. Außerdem haben wir den oben behandelten Fall einer Verarbeitung auf Basis einer Einwilligung hier ausgeschlossen.

Ob diese Folgerung wirklich zulässig ist, ist umstritten, aber nach Einschätzung der Autoren gibt es gute Argumente diese Ansicht zu vertreten.

2.4 Vereinbarkeit des Testens mit dem ursprünglichen Verarbeitungszweck

2.4.1 Vereinbarkeitsprüfung

Wenn der Test nicht Bestandteil des ursprünglich definierten Zwecks ist, erlaubt der Grundsatz der Zweckbindung (Art. 5 Abs. 1 lit b) i.V.m. Art. 6 Abs. 4 DSGVO eine Zweckänderung, wenn der neue Zweck mit dem ursprünglichen Zweck vereinbar ist.[3] Der Grundsatz der Zweckbindung ist daher nicht ganz korrekt benannt, da er nicht wirklich eine Zweckbindung fordert, sondern eine Zweckvereinbarkeit.

Um zwischen den oben eingeführten Fällen 3 und 4 und den daraus folgenden Konsequenzen zu unterscheiden, ist also eine Prüfung erforderlich, ob der neue Zweck des Testens mit dem ursprünglich definierten Zweck der Verarbeitung vereinbar ist. Die dafür anzuwendenden Kriterien sind in Art. 6 Abs. 4 DSGVO wie folgt definiert:

Zur Feststellung, ob der neue Verarbeitungszweck mit dem ursprünglichen vereinbar ist, berücksichtigt der Verantwortliche „*unter anderem a) jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung, b) den Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen, c) die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten gemäß Artikel 9 verarbeitet werden oder ob personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 verarbeitet werden, d) die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen, e) das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann.*"

Zu beachten ist, dass diese Kriterienliste nicht abschließend ist und außerdem die Kriterien erheblichen Interpretationsspielraum erlauben. Im Folgenden soll daher die genannten Kriterien im Kontext des Softwaretests mit Originaldaten näher untersucht werden.

2.4.2 Bedeutung der Kriterien beim Softwaretest

Kriterium a) betrachtet die Verbindung zwischen den ursprünglichen Zwecken der Datenerhebung und den Zwecken der Weiterverarbeitung, hier also des Testens. Eine enge Verbindung besteht, wenn das zu testende System dem gleichen Zweck wie die ursprüngliche Verarbeitung dient, es sich also um eine Weiterentwicklung, Fehlerkorrektur oder Migration auf eine neue technische Basis handelt. Handelt es sich dagegen um eine Entwicklung komplett neuer Funktionalität, so ist die Verbindung entsprechend geringer.

Kriterium b) betrachtet den Kontext, in dem die Originaldaten erhoben wurden, und die Frage, ob es den vernünftigen Erwartungen der Betroffenen entspricht, die erhobenen Daten auch für den Test zu verwenden. Wenn beispielsweise bei den Informationen gemäß Art. 13 bzw. 14 DSGVO eine sehr restriktive Zweckbindung beschrieben wurde, wird eine Nutzung für den Test den vernünftigen Erwartungen eher widersprechen. Soweit das nicht der Fall ist, wird zwar kaum ein Betroffener bei der Information über die ursprüngliche Verarbeitung daran denken, dass auch ein IT-System entwickelt und getestet werden muss, um diese Verarbeitung durchzuführen, aber es wird i. A. auch nicht im Widerspruch zu seinen Erwartungen stehen.

In Kriterium c) ist die Art der personenbezogenen Daten zu berücksichtigen. Handelt es sich bei den für den Test zu nutzenden Originaldaten um personenbezogene Daten besonderer Kategorien, um Daten über strafrechtliche Verurteilungen oder um Daten von Kindern, dann ist eine Vereinbarkeit des Testens in der Regel zu verneinen.

Speziell für den Fall der personenbezogenen Daten besonderer Kategorien kommt dazu, dass hier die ursprüngliche Verarbeitung gemäß Art. 9 DSGVO oft auf einer Einwilligung basiert, und in diesem Fall sind die Vereinbarkeitskriterien nicht anwendbar.[4] Für das oben eingeführte Beispiel des Tests einer Datenmigration in ein neues Kernsystem einer Versicherung bedeutet das, dass der Test mit Originaldaten in der Regel nicht mit dem ursprünglichen Zweck vereinbar ist.

Kriterium d) betrachtet die Folgen der Nutzung von Originaldaten beim Testen für die Betroffenen. Negative Folgen können weitgehend minimiert werden, sofern sichergestellt wird, dass der Zugriff auf die im Test verwendeten Originaldaten angemessen restriktiv gehandhabt und die Daten vor unberechtigtem Zugriff geschützt sind. Umgekehrt hat ein gründlicher Test sogar positive Auswirkungen auf die Betroffenen, da damit die Wahrscheinlichkeit einer Fehlfunktion des Systems und damit von Fehlern bei der Verarbeitung ihrer Daten reduziert wird.

3 Ob dafür eine neue Rechtsgrundlage erforderlich ist, ist umstritten, siehe Kap. 5.1.

4 Diese Argumentation geht davon aus, dass „Verarbeitung" in Art. 6 Abs. 4 Satz 1 DSGVO sich auf die ursprüngliche Verarbeitung bezieht, nicht auf die neue, dem geänderten Zweck dienende Verarbeitung. Das ist aber in der DSGVO nicht eindeutig formuliert und wird teilweise auch anders interpretiert.

Schließlich fordert Kriterium e) die Berücksichtigung geeigneter Garantien, wozu in diesem Fall insbesondere restriktive Zugangskontrollen gehören. Dagegen sind die beispielhaft genannten Garantien einer Verschlüsselung oder Pseudonymisierung hier nicht geeignet. Eine Verschlüsselung würde die Nutzung der Daten für den Test verhindern, während eine Pseudonymisierung, wie oben erläutert, beim Test immer durch eine Anonymisierung ersetzt werden sollte.

2.4.3 Sonderfall: Verarbeitung zu Archiv-, Forschungs- oder statistischen Zwecken

Neben einer Verarbeitung personenbezogener Daten zu einem anderen Zweck als dem ursprünglich vorgesehenen nach Art. 6 Abs. 4 DSGVO, bietet Art. 5 Abs. 1 lit. b i. V. m. Art. 89 Abs. 1 DSGVO eine zusätzliche Rechtsgrundlage für Weiterverarbeitungen für Archiv- oder Forschungszwecke:

„… eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung");"

Einer gesonderten Kompatibilitätsprüfung bedarf es in diesen Fällen nicht, allerdings ist dieser Sonderfall für den hier betrachteten Softwaretest kaum relevant.

3 Ursprüngliche Verarbeitung auf Basis einer Einwilligung

Sofern die ursprüngliche Verarbeitung auf der Rechtsgrundlage einer Einwilligung stattfindet, die u. a. durch ihre Bestimmtheit gekennzeichnet ist, kann die Nutzung der personenbezogenen Daten für den Test nur dann Bestandteil des ursprünglichen Verarbeitungszwecks sein, wenn diese Nutzung explizit in der Einwilligung benannt ist – eine Konstellation, die praktisch wohl nur in Ausnahmefällen vorkommen wird. Ist das aber der Fall, dann ist auch eine Rechtsgrundlage für den Test vorhanden und eine zusätzliche Information der Betroffenen nicht erforderlich, da sie schon beim Einholen der Einwilligung erfolgt sein muss.

Bis auf den genannten Ausnahmefall ist die Nutzung der Originaldaten für den Test aber nicht möglich bzw. benötigt sie eine neue, eigene Einwilligung. Da aber viele Betroffene eine solche Einwilligung nicht erteilen werden, kommt eine Nutzung der Originaldaten in diesem Fall nicht in Frage, zumal dabei noch berücksichtigt werden müsste, dass eine erteilte Einwilligung möglicherweise wieder zurückgezogen wird.

4 Test als Bestandteil des ursprünglichen Zwecks

Der Test als Bestandteil des ursprünglich definierten Zwecks ist aus Datenschutzsicht am einfachsten zu behandeln. In diesem Fall ist die Rechtsgrundlage für die Nutzung der Originaldaten für den Test bereits vorhanden, und auch eine separate Information der Betroffenen ist nicht erforderlich.

Ist man sich daher von Anfang an bewusst, dass die Daten auch für Tests eingesetzt werden sollen, sollte man dies bereits zu Beginn bei der Information der Betroffenen berücksichtigen, und die Nutzung zum Test ist damit unproblematisch.

5 Test als mit dem ursprünglichen Zweck vereinbare Verarbeitung

5.1 Notwendigkeit einer Rechtsgrundlage bei einer kompatiblen Zweckänderung

Umstritten ist, ob neben dem beschriebenen Kompatibilitätstest bei einer kompatiblen Zweckänderung noch weitere Voraussetzungen zu erfüllen sind. Verlangt wird teilweise, dass zusätzlich zu den Kriterien nach Art. 6 Abs. 4 DSGVO auch die allgemeinen Voraussetzungen der Verarbeitung personenbezogener Daten nach Art. 6 Abs. 1 DSGVO zu erfüllen sind, da jede Verarbeitung nach Art. 5 Abs. 1 DSGVO rechtmäßig sein muss.[5] Dies steht jedoch im Widerspruch zu den Vorgaben der DSGVO in Erwägungsgrund 50 S. 2, der besagt, dass gerade „keine andere gesonderte Rechtsgrundlage erforderlich ist als diejenige für die Erhebung der personenbezogenen Daten".

Gegen die Forderung nach einer eigenen Rechtsgrundlage für die kompatible Weiterverarbeitung spricht, dass sie im Fall einer Zweckänderung zu höheren rechtlichen Anforderungen führt als bei der ursprünglichen Verarbeitung, nämlich sowohl der Zweckvereinbarkeit als auch einer Rechtsgrundlage gemäß Art. 6 Abs. 1 DSGVO.

Da derzeit unklar ist, welche rechtliche Meinung sich durchsetzen wird, gehen wir im Folgenden davon aus, dass eine zusätzliche Rechtsgrundlage erforderlich ist. Sollte das nicht der Fall sein, entfällt die in Abschnitt 5.2 beschriebene Prüfung der Rechtmäßigkeit.

5.2 Rechtsgrundlage

Als Rechtsgrundlage für den Softwaretest mit Originaldaten kommt, bis auf seltene Sonderfälle, praktisch nur das berechtigte Interesse nach Art. 6 Abs. 1 lit. f DSGVO in Frage. Um die Rechtsgrundlage des berechtigten Interesses anwenden zu dürfen, müssen folgende Checkpunkte überprüft werden:[6]

- Berechtigtes Interesse: Hat der Verantwortliche ein berechtigtes Interesse an der Nutzung der Originaldaten für den Test?
- Erforderlichkeit: Ist die Nutzung der Daten erforderlich (und nicht nur nützlich) für den angestrebten Zweck der Verarbeitung?
- Interessenabwägung: Überwiegen die Interessen des Verantwortlichen auf Nutzung der Originaldaten für den Test die Interessen der Betroffenen, dass ihre Daten nicht für diesen Zweck eingesetzt werden?

5.2.1 Berechtigtes Interesse

Ein berechtigtes Interesse des Verantwortlichen, die Software gründlich zu prüfen, liegt offensichtlich vor.

5.2.2 Erforderlichkeit

Um sich auf die wirklich erforderliche Verarbeitung zu beschränken, den Grundsatz der Datenminimierung umzusetzen und die Auswirkungen möglichst gering zu halten, muss der Zugriff auf die Testdaten sehr restriktiv gehandhabt werden, und es müssen geeignete technische und organisatorische Maßnahmen umge-

5 Diese Ansicht vertreten beispielsweise *Herbst* sowie *Buchner* und *Petri* in [3], Art. 5 Rn 48f, Art. 6 Rn 181-183.

6 Siehe [4], S. 11

setzt werden, so dass nur diejenigen Personen Zugriff auf die Testdaten bekommen, die diesen wirklich benötigen.

In einigen Fällen ist sogar ein externer Nachweis des gründlichen Tests der Software, evtl. gegenüber einer Aufsichtsbehörde, gefordert. Dies gilt beispielsweise bei der bereits angesprochenen Datenmigration in ein neues Kernsystem einer Versicherung, und in einem solchen Fall liegt ein hoher Grad der Erforderlichkeit eines Tests mit Originaldaten vor.

5.2.3 Interessenabwägung

Soweit die genannten Maßnahmen zur Minimierung der Auswirkungen umgesetzt sind, wird es meist aus Sicht der Betroffenen keine gravierenden Gründe geben, die gegen eine solche Nutzung sprechen, auch wenn Ausnahmen und Sonderfälle natürlich immer möglich sind. Im Gegenteil ist es ja sogar meist im Interesse der Betroffenen, dass das System, mit dem ihre Daten verarbeitet werden, gründlich getestet wird und später korrekt funktioniert.

5.2.4 Zusammenfassung

Wenn der hier betrachtete Fall vorliegt und der Test mit Originaldaten eine mit dem ursprünglichen Zweck vereinbare Verarbeitung darstellt, dann ist die Erforderlichkeit dieser Tests sicherzustellen, was im Wesentlichen aber bereits bei der Prüfung der Zweckvereinbarkeit überprüft wurde.

Ergänzend dazu muss die IT-Sicherheit der Daten durch geeignete technische und organisatorische Maßnahmen, insbesondere Zugriffsbeschränkungen, sichergestellt werden.

5.3 Informationspflicht

Gemäß Art. 13 Abs. 3 DSGVO bzw. Art. 14 Abs. 4 DSGVO besteht eine Informationspflicht des Verantwortlichen gegenüber den Betroffenen bei einer (erlaubten) Zweckänderung. Im konkreten Fall bedeutet das, dass der Verantwortliche den Betroffenen Informationen über die geplante Nutzung ihrer Daten für den Test zur Verfügung stellen muss, zusätzlich zur ursprünglichen Information über die ursprünglich geplante Verarbeitung dieser Daten. Diese Forderung gilt unabhängig davon, ob für den Test eine eigene Rechtsgrundlage erforderlich ist oder nicht.

Das stellt in der Praxis eine erhebliche Herausforderung dar, denn es handelt sich typischerweise um eine Vielzahl von Betroffenen, und nicht immer liegen entsprechende Kontaktdaten vollständig vor.

6 Test als nicht mit dem ursprünglichen Zweck vereinbare Verarbeitung

Wenn der Test mit Originaldaten nicht mit dem ursprünglichen Zweck vereinbar ist, dann ist dafür sicher eine eigene Rechtsgrundlage erforderlich, bei der es sich aber, analog Abschnitt 5.2, um das berechtigte Interesse handeln könnte.

Unklar ist, ob dafür eine neue Erhebung der Daten erforderlich ist, was diesen Test in den meisten Fällen praktisch unmöglich machen würde. Das führt zurück zu der in Abschnitt 5.1 diskutierten Notwendigkeit einer eigenen Rechtsgrundlage für eine kompatible Verarbeitung.

- Angenommen es ist eine eigene Rechtsgrundlage für eine kompatible Verarbeitung erforderlich. Dann kann alleine eine neue Rechtsgrundlage für die nicht kompatible Verarbeitung nicht ausreichen, da sonst die Vereinbarkeitsprüfung überflüssig wäre. Hier ist also davon auszugehen, dass eine Verarbeitung der bestehenden Daten trotz der neuen Rechtsgrundlage nicht erlaubt wäre, sondern die Daten neu erhoben werden müssen.
- Ist dagegen für eine kompatible Verarbeitung keine eigene Rechtsgrundlage erforderlich, so führt die fehlende Vereinbarkeit dazu, dass eine Rechtsgrundlage für den neuen Zweck, hier also den Test mit Originaldaten, erforderlich wird. In diesem Fall ist davon auszugehen, dass die Vereinbarkeitsprüfung genau für diese Unterscheidung gedacht ist und bei einer vorhandenen neuen Rechtsgrundlage die Originaldaten ohne Neuerfassung genutzt werden dürfen.

7 Zusammenfassung

Ein Test mit Originaldaten ist unter sehr restriktiven Voraussetzungen und Rahmenbedingungen möglich, auch wenn er gemäß dem Grundsatz der Datenminimierung nach Möglichkeit vermieden werden sollte. Wichtigste Voraussetzungen sind, dass der Testzweck nicht mit fiktiven oder anonymisierten Daten erreichbar ist, dass die ursprüngliche Verarbeitung auf einer anderen Rechtsgrundlage als einer Einwilligung basiert und dass der Test sehr direkt diese ursprüngliche Verarbeitung unterstützt, idealerweise einen Bestandteil des ursprünglichen Verarbeitungszwecks bildet, sowie die zusätzlichen Risiken für die Betroffenen möglichst gering gehalten werden, insbesondere durch geeignete technische und organisatorische Maßnahmen zur IT-Sicherheit und restriktive Zugriffsbeschränkungen.

Literatur

[1] Der Hamburgische Datenschutzbeauftragte. Tätigkeitsbericht 2006/2007. S. 24f. https://datenschutz-hamburg.de/assets/pdf/21._Taetigkeitsbericht_2006-2007.pdf
[2] Datenschutz-Wiki-Bearbeiter Softwaretest mit Echtdaten, Datenschutz-Wiki, https://www.datenschutz-wiki.de/index.php?title=Softwaretest_mit_Echtdaten&oldid=2794 (abgerufen am 25. November 2020).
[3] Kühling / Buchner. DS-GVO BDSG Kommentar. 3. Aufl., 2020, Verlag C.H. Beck.
[4] Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK). Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien. März 2019.