Datenschutzrechtliche Betrachtung

Projekt ITS.APT – Dokument 2.3

Autoren:

Dr.-Ing. Meiko Jensen

Hannah Obersteller

für das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

Das Projekt erhält Förderung durch das Bundesministerium für Bildung und Forschung.

Inhalt

A. Einleitung

I. Zum Projekt

Infrastrukturen der Informationstechnik (IT) werden immer häufiger das Ziel von Cyberattacken, mit teils großen wirtschaftlichen und ideellen Schäden. Möglich sind in etwa Beeinträchtigungen des Betriebs der betroffenen Institution, sowie Datenverluste, die die Reputation beeinträchtigen oder gar Haftungsfälle generieren. Denkbar ist außerdem der Verlust von personenbezogenen Informationen und Betriebsgeheimnissen. Besonders gravierend sind die Folgen eines solchen Angriffs dann, wenn kritische Infrastrukturen, wie Krankenhäuser, Versorgungs- oder Verkehrseinrichtungen betroffen sind, da diese eine besonders wichtige Bedeutung für das staatliche Gemeinwesen haben.

Zur Bewertung der IT-Sicherheit in Unternehmen werden in die Regel sog. penetration tests durchgeführt. IT-Sicherheitsdienstleister versuchen dabei in das IT System einzudringen, um Sicherheitsschwachstellen oder Lücken zu ermitteln, die dann geschlossen werden können. Die Überprüfung der Verwundbarkeit von IT-Infrastrukturen ist dabei jedoch regelmäßig auf Aspekte der technischen Sicherheit limitiert. Außen vor bleiben Risiken, die auf Seiten der Nutzer des Systems entstehen, indem sie bspw. unangemessen auf Sicherheitshinweise reagieren

Dieses Defizit ist der Ausgangspunkt eines neuen vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Verbundprojekts „IT-Security Awareness Penetration Testing" (ITS.APT), das es sich zum Ziel gesetzt hat, das IT Sicherheitsbewusstsein der Nutzer eines IT Systems zu messen und Wege zu finden, es zu verbessern. Dazu wird eine Software entwickelt, die IT-Attacken auf das Computersystem, wie Phishing Mails oder sog. SQL-Injections, simuliert. Der Nutzer nimmt diese in Form von angezeigten Artefakten, also fremd anmutenden Anzeigen auf dem Bildschirm, wahr. Die Reaktionen der Nutzer auf die IT-Angriffe werden, ebenfalls mittels der Software, protokolliert und können schließlich Erkenntnisse über deren IT-Sicherheitsbewusstsein liefern. Beispielsweise spricht das direkte Löschen einer Phishing E-Mail eher für ein erhöhtes Sicherheitsbewusstsein, während das Anklicken eines Links in der Phishing E-Mail eher für das Gegenteil spricht.

In einem groß angelegten Feldtest am Universitätsklinikum Schleswig-Holstein (UKSH) sollen die Arbeitnehmer des Klinikums als Nutzer der dortigen IT Systeme getestet werden. Der Test findet dabei unter normalen Arbeitsbedingungen statt, um möglichst authentische Ergebnisse zu gewährleisten. Die Maßnahme wird zuvor entsprechend der geltenden gesetzlichen Bestimmungen mit dem Personalrat (PR) abgestimmt und in einer den

Mitarbeitern zugänglichen Dienstvereinbarung transparent beschrieben. Im Anschluss an diesen ersten Test sollen die Nutzer gezielt, aber unterschiedlich auf das Bemerken von IT Angriffen geschult werden. Anschließend wird die gleiche Testgruppe wiederum durch simulierte IT Angriffe getestet, um zu evaluieren, welche Schulungsmaßnahme am effektivsten ist und das IT Sicherheitsbewusstsein am besten steigert.

II. Zum Dokument

Die zur Testdurchführung entwickelte Software muss in das IT-System des UKSH eingebracht werden. Neben der Beachtung reiner Datensicherheitsaspekte, müssen dabei selbstverständlich auch und gerade die einschlägigen datenschutzrechtlichen Bestimmungen eingehalten werden. Im Hinblick auf die anvisierte Testdurchführung im laufenden Betrieb und Alltag des UKSH, sind rechtliche und praktische Grenzen aufzuzeigen, um das Risiko von Datenpannen zu minimieren. In diesem Dokument werden vertieft die einschlägigen Normen des Datenschutzrechts aus Telekommunikationsgesetz (TKG) und Landesdatenschutzgesetz Schleswig Holstein (LDSG), sowie ergänzend die Normen des Bundesdatenschutzgesetzes (BDSG) betrachtet und die sich daraus ergebenden Konsequenzen für die Testdurchführung zusammengefasst. Hierzu wird zunächst die Datenschutzrelevanz der Angriffsszenarien vertieft dargestellt (Kapitel B.), d.h. Ausführungen zu den zu Testzwecken zu erhebenden Kategorien von Daten und der im UKSH gegebene rechtliche wie organisatorische Rahmen. Darauf aufbauend werden der rechtliche Rahmen abgesteckt (Kapitel C.) und die Rechtsgrundlagen für die Testdurchführung aus Datenschutzsicht erörtert (Kapitel D.), wobei auch ein Ausblick auf die Datenschutz-Grundverordnung genommen und angesprochen wird, inwiefern sich datenschutzrechtliche Folgen aus dem IT-Sicherheitsgesetz, bzw. der einschlägigen Rechtsverordnung ergeben können. In Kapitel F. wird sodann aufbauend auf die rechtlichen Erwägungen die technische Durchführung dargestellt und auf besondere Herausforderungen hingewiesen. Kapitel G. beschäftigt sich mit den datenschutzrechtlich zu gewährleistenden Betroffenenrechten. Abschließend wird in Kapitel H. angesprochen, inwiefern die Voraussetzungen der Testdurchführung auf andere Szenarien übertragbar sind, bzw. inwieweit aus derzeitiger Sicht bereits ein potenzieller Praxiseinsatz beurteilt werden kann. Das Dokument berücksichtigt den Stand der technischen Entwicklung im Projekt von April 2016. Bei Feststehen aller Artefakte, wird – soweit erforderlich – ein Zusatzdokument zu Teilarbeitspaket 2.3 erstellt, das die neuen technischen Entwicklungen betrachtet, bzw. die hier zunächst allgemein gehaltenen Ausführungen präzisiert.

B. Datenschutzrelevanz der Angriffsszenarien

Zum besseren Verständnis sollen zunächst die Projektziele und –stufen nochmals zusammengefasst werden: Gegenstand der im Projekt ITS.APT geplanten Arbeiten ist die Durchführung eines experimentellen Ansatzes zur Erfassung, Messung und Auswertung des Sicherheitsbewusstseins von Mitarbeitern am UKSH. Zu diesem Zweck werden verschiedene Aktivitäten durchgeführt, die die hierfür erforderlichen Daten generieren. Das Experiment unterteilt sich hierbei in drei Stufen:

- In der ersten Stufe werden Mitarbeiter des UKSH (sog. *Probanden*) gezielt in Situationen versetzt, die eine Reaktion auf Basis ihres jeweiligen IT-Sicherheitsbewusstseins erzeugen. Beispielsweise werden sie an ihrem Arbeitsplatz-Computer mit einer Warnmeldung eines Antivirusprogrammes konfrontiert, mit einer eingehenden Phishing-E-Mail, einer selbsttätig startenden bildschirmfüllenden Videowiedergabe oder mit einem anderweitigen anormalen Verhalten. Die jeweiligen Reaktionen der Probanden auf diese künstlich erzeugten IT-Sicherheitsvorfälle werden protokolliert.
- In der zweiten Stufe erhalten die Probanden eine gezielte Schulung in Hinblick auf IT-Sicherheit am Arbeitsplatz, die auch jene Anormalitäten thematisiert, denen die Mitarbeiter in der ersten Stufe ausgesetzt wurden.
- In der dritten Stufe werden die nun geschulten Probanden erneut mit IT-Sicherheitsrelevanten Anomalien am Arbeitsplatz konfrontiert. Wie in der ersten Stufe werden dabei die Reaktionen der Probanden protokolliert.

Aus den derart gewonnenen Daten sollen dann im Nachgang Erkenntnisse über Art und Qualität des Erfolges von Schulungsmaßnahmen zur Schärfung des IT-Sicherheitsbewusstseins bei den Probanden gewonnen werden.

I. Personenbezogene Daten

Das Datenschutzrecht zielt darauf ab, den „Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird“ (§ 1 LDSG; § 1 Abs. 1 BDSG[1]). Es findet dementsprechend nur auf die Verarbeitung personenbezogener Daten Anwendung (vgl. etwa § 1 Abs. 2 S. 1 BDSG). Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (§ 2 Abs. 1 LDSG). Einzelangaben sind hierbei Informationen, die sich auf eine bestimmte natürliche Person beziehen oder geeignet sind, einen Bezug zu ihr

[1] Für das UKSH gilt gem. § 3 Abs. 1 LDSG das Landesdatenschutzgesetz Schleswig Holstein. Mit Blick auf eine bessere Verwertbarkeit dieses Gutachtens auch durch Rezipienten aus dem Bereich der Wirtschaft werden auch die jeweils einschlägigen Normen des BDSG mit genannt. In Ermangelung aktueller Kommentarliteratur zum LDSG werden die Kommentierungen zu den inhaltsgleichen Normen des BDSG herangezogen.

herzustellen.[2] Wenn sich ein Datum also nicht direkt einer (bestimmten) Person zuordnen lässt, liegt dennoch per Definition ein Personenbezug vor, wenn die Person „bestimmbar“ ist. In der juristischen Literatur wird diesbezüglich die Frage aufgeworfen, ob die Person an Hand der vorliegenden Daten „objektiv“ oder „relativ“ bestimmbar sein muss, um von einem personenbezogenen Datum auszugehen.[3] Objektive Bestimmbarkeit der Person meint, dass die Person allgemein – für eine beliebige Stelle – identifizierbar ist. Es kommt nicht nur auf die Kenntnisse, Mittel und Möglichkeiten der datenverarbeitenden Stelle an. Ein Personenbezug besteht erst dann nicht, wenn Einzelangaben von niemandem oder aber nur mit einem unverhältnismäßig großen Zeit-, Kosten- und Arbeitsaufwand (geleistet durch eine beliebige Stelle) einer natürlichen Person zuzuordnen wären.[4] Relative Bestimmbarkeit der Person hingegen stellt auf die Kenntnisse, Mittel und Möglichkeiten der konkreten datenverarbeitenden Stelle ab. Hiernach besteht ein Personenbezug schon nicht, wenn die Einzelangaben von dieser Stelle nicht oder nur mit einem unverhältnismäßig großen Zeit-, Kosten- und Arbeitsaufwand einer natürlichen Person zugeordnet werden könnte.[5] In der Folge würden damit pseudonymisierte Daten, für die ausschließlich eine Dritte Stelle die Zuordnung zu einer Person herstellen kann, anonymisierten Daten gleichgestellt. Für die Übermittlung und weitere Verarbeitung zwischen öffentlichen Stellen in Schleswig-Holstein ist ein solcher Ansatz § 1 Abs. 6 LDSG zu entnehmen, der eine Weiterverarbeitung pseudonymisierter Daten durch eine andere öffentliche Stelle ermöglicht, soweit die Zuordnungsfunktion im alleinigen Zugriff der übermittelnden Stelle verleibt.

Im Hinblick auf die zunehmenden technischen Möglichkeiten der automatisierten Datenverarbeitung ist es technisch kaum noch denkbar, dass effektiv niemand in der Lage sein würde, einen Personenbezug (wieder)herzustellen. Vgl. hierzu sogleich unter V.

Grundrechtlich ist das Datenschutzrecht auf das Recht der Einzelnen, selbst über „Preisgabe und Verwendung der ihre Person betreffenden Daten zu entscheiden“ gestützt.[6] Das sog. Recht auf informationelle Selbstbestimmung wurde erstmals 1983 durch das „Volkszählungsurteil“ des Bundesverfassungsgerichts (BVerfG) als Teil des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 i.V.m. Art. 1 GG abgeleitet.[7]

[2] Gola/Schomerus/, BDSG, § 3 Rn. 3.
[3] Vgl. hierzu auch (im Zusammenhang mit Pseudonymen) Dokument 2.1 „Arbeitsrechtliche Betrachtung“.
[4] Däubler/Klebe/Wedde/Weichert/*Weichert*, BDSG, § 3 Rn. 13.
[5] Gola/Schomerus/*Gola/Klug/Körffer*, BDSG, § 3 Rn. 10.
[6] Simitis/*Simitis*, BDSG, § 1 Rn. 46.
[7] BVerfG, Urteil vom 15. Dezember 1983, Az. 1 BvR 209/83, 1 BvR 484/83, 1 BvR 440/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83.

II. Kategorien von Daten

Im Hinblick auf personenbezogene Daten können je nach Art und Verarbeitungszusammenhang verschiedene Rechtsnormen, auch verortet in verschiedenen Gesetzen,[8] relevant werden. Im Folgenden sollen einige Kategorien von Daten kurz im Hinblick auf die sich für die Testdurchführung ergebenden Besonderheiten beleuchtet werden.

1. Medizin-/Gesundheits-/Patientendaten

§ 3 Abs. 9 BDSG definiert sog. „besondere Arten personenbezogener Daten“ als Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Im LDSG S-H findet sich eine entsprechende Regelung in § 11 Abs 3 LDSG S-H, erweitert um die Daten, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen. In einem Krankenhauses wird insbesondere mit Gesundheitsdaten umgegangen.

Gemeinsam genannt mit u.a. Daten über politische Meinungen und religiöse Überzeugungen werden Gesundheitsdaten einem besonderen Schutz unterstellt. Die besondere Schutzbedürftigkeit von Gesundheitsdaten – oder wie das Gesetz formuliert: „Angaben über die Gesundheit“ i.S.d. § 3 Abs. 9 BDSG bzw. „personenbezogene Daten über die Gesundheit“ i.S.d. § 11 Abs. 3 LDSG S-H – ist in den Datenschutzgesetzen festgeschrieben. Diese Regelungen basieren auf Art. 8 der Europäischen Datenschutzrichtlinie,[9] der den Besonderen Schutz dieser Daten begründet. [10] Dieser äußert sich in erster Linie darin, dass etwa gesetzlich strengere Voraussetzungen an die Einwilligung als Grund zur Datenerhebung und –verarbeitung gestellt werden (vgl. § 4a BDSG, §§ 12, 13 Abs. 4 LDSG S-H) und an Abwägungsvorgänge (vgl. etwa § 28 Abs. 6 BDSG).

Wenn Daten einer dieser Kategorien zuzuordnen sind, sind sie als sensibel zu betrachten. Eine Ansehung des einzelnen Datums findet nicht mehr statt. Irrelevant für die Einordnung in eine dieser Gruppen ist, ob das Datum explizit sensibel ist – wie etwa konkrete Werte aus einer Patientenakte – oder ob sich die Sensibilität aus dem Gesamtzusammenhang ergibt.[11] So ist z.B. bereits die Tatsache, dass jemand bei einem bestimmten Arzt in Behandlung ist, ein medizinisches Datum.

---

[8] Vgl. hierzu sogleich unter III.
[9] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr; Amtsblatt Nr. L 281 vom 23.11.1995 S. 0031-0050.
[10] Däubler/Klebe/Wedde/Weichert/*Weichert*, BDSG, § 3 Rn. 65.
[11] Gola/Schomerus/*Gola/Klug/Körffer*, BDSG, § 3 Rn. 56.

Flankierend stehen Gesundheitsdaten auch unter dem besonderen Schutz anderer Rechtsnormen. Die Offenbarung von anvertrauten Informationen ist für Angehörige der Heilberufe, insbesondere Ärzte, und deren Mitarbeiter strafbewährt (§ 203 StGB). Die Berufsordnungen der Landesärztekammern normieren die Schweigepflicht und sanktionieren Verstöße. Schließlich bestehen auch aus dem zivilrechtlichen Behandlungsvertrag Unterlassungs- und Schadensersatzansprüche bei unberechtigter Weitergabe von Patientendaten.

Obwohl für die Projektdurchführung keine Gesundheitsdaten (oder sonstige Daten i.S.d. § 11 Abs. 3 LDSG S-H) erheben werden, ist zu berücksichtigen, dass die Tests im Umfeld eines Krankenhauses und unter Einbeziehung seines IT-Systems stattfinden. Von der Überlegung, Screenshots oder Screencasts von den Bildschirmen der Probanden anzufertigen um Reaktionen besser dokumentieren zu können und diese den UKSH-externen Projektpartnern zur Verfügung zu stellen, musste daher v.a. aus Gründen des Patientendatenschutzes Abstand genommen werden. Es besteht die Gefahr, dass neben den durch die Testdurchführung erzeugten Artefakten auch Dokumente geöffnet und auf dem Bildschirm sichtbar sind, die Gesundheitsdaten von Patienten enthalten. Die Übermittlung eines Screenshots an Projektpartner würde dementsprechend unzulässiger Weise solche Daten Dritten offenbaren. Bei der Testdurchführung ist zudem insbesondere § 203 StGB zu beachten. (Siehe dazu sogleich unter D. II.)

2. Arbeitnehmerdaten – Verkehrs- und Personaldaten

Die arbeits- und auch datenschutzrechtlichen Besonderheiten, die sich aus der Testdurchführung mit Arbeitnehmern an ihren tatsächlichen Arbeitsplätzen ergeben, werden in dem Dokument 2.1 „Arbeitsrechtliche Betrachtung“ schwerpunktmäßig ausgeführt.

3. Daten i.S.d. §§ 5, 6 LDSG S-H

Aus Gründen der IT-Sicherheit, ist es den datenverarbeitenden Stellen gestattet, bestimmte Daten zu „loggen“, d.h. zu speichern. Hierbei handelt es sich insbesondere um sog. „Protokolldaten“, die bspw. für Zugriffe berechtigter Personen, die Änderungen an automatisierten Verfahren bewirken können, zu speichern sind (§ 6 Abs. 2 LDSG S-H) oder im Fall ausschließlich automatisierter Speicherung, Veränderung und Übermittlung personenbezogener Daten wann, durch wen und in welcher Weise die Verarbeitungen vorgenommen wurden. Für diese Protokolldaten ist gem. § 6 Abs. 4 S. 3 LDSG S-H vorgesehen, dass sie mit den jeweils betroffenen Daten sichtbar gemacht werden können und den gleichen Aufbewahrungsfristen unterliegen. Gründe für diese weitgehende Erlaubnis und

Pflicht zur Protokollierung sind v.a. die Gewährleistung der Transparenz, einer Kontrollmöglichkeit der Handlungen von System-Administratoren, sowie die Sicherstellung der jederzeitigen Möglichkeit des Lesens, bzw. der Wiederherstellung, noch (gesetzlich) erforderlicher Daten, auch wenn über diese keine papierene Unterlagen mehr existieren.[12] Für die nach §§ 5, 6 LDSG S-H erhobenen und gespeicherten Daten besteht ein absolutes Verwendungsverbot für Zwecke der Verhaltens- oder Leistungskontrolle im Rahmen von Beschäftigungsverhältnissen (§ 23 Abs. 2 LDSG S-H).

C. Anwendbares Recht

Allgemeine Datenschutzgesetze existieren in Deutschland auf Bundes-, sowie auf Länderebene (zur Anwendbarkeit vgl. sogleich III.). Sie dienen jeweils der Umsetzung der europäischen Richtlinie 95/46/EG des europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.[13] Die allgemeinen Datenschutzgesetze sind indes lediglich subsidiär anzuwenden, d.h. nur soweit keine spezielleren Regelungen für den zu beurteilenden Sachverhalt existieren.[14] In § 1 Abs. 3 des Bundesdatenschutzgesetzes oder § 3 Abs. 3 des Landesdatenschutzgesetzes Schleswig-Holstein finden sich entsprechende Subsidiaritätsklauseln. Vorrangig gelten bereichsspezifische Regelungen. Soweit es um die Verarbeitung personenbezogener Daten im Rahmen von sog. Telekommunikations- und Telemediendiensten geht, gehen das Telekommunikations-, bzw. das Telemediengesetz vor.[15]

1. BDSG und LDSG

Ob das Bundesdatenschutzgesetz oder eines der Landesdatenschutzgesetze auf einen Sachverhalt anzuwenden ist, bestimmt sich nach der Organisationsform der (für die Datenverarbeitung) „verantwortlichen Stelle“, sowie ggf. ihren Sitz. „Verantwortliche Stelle“ ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt (§ 3 Abs. 7 BDSG).

Die deutschen Datenschutzgesetze von Bund wie Ländern unterscheiden öffentliche von nicht-öffentlichen Stellen und regeln deren jeweilige Verantwortlichkeiten in Bezug auf die Verarbeitung personenbezogener Daten in verschiedenen Abschnitten.

---

[12] Vgl. insofern zu den Vorgängervorschriften (§§ 6, 7 LDSG S-H a.F.): https://www.datenschutzzentrum.de/material/recht/ldsg-novellierung/begruend.htm#Par6

[13] Online verfügbar: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:DE:HTML.

[14] Simitis/*Dix*, BDSG, § 1 Rn. 158.

[15] Spindler/Schuster/*Eckhardt*, 11. Teil § 91, Rn. 2; Spindler/Schuster/*Spindler/Nink*, 12. Teil § 12, Rn. 1.

Für öffentliche Stellen des Bundes gilt das BDSG. Dies sind die Behörden, Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes, der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform (§ 2 Abs. 1 S. 1 BDSG). Für öffentliche Stellen der Länder gilt das jeweilige LDSG.[16] Hierbei handelt es sich um die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen eines Landes, einer Gemeinde, eines Gemeindeverbandes und sonstiger der Aufsicht des Landes unterstehender juristischer Personen des öffentlichen Rechts sind, sowie deren Vereinigungen ungeachtet ihrer Rechtsform (§ 2 Abs. 2 BDSG). Vereinigungen des privaten Rechts des Bundes oder der Länder, die Aufgaben der öffentlichen Verwaltung wahrnehmen können – auch bei Beteiligung nicht-öffentlicher Stellen – ebenso als öffentliche Stellen gelten. Sie gelten als öffentliche Stellen des Bundes, wenn sie entweder über den Bereich eines Landes hinaus tätig werden oder dem Bund die absolute Mehrheit der Anteile gehört oder ihm die absolute Mehrheit der Stimmen zusteht. Andernfalls gelten sie als öffentliche Stellen der Länder (§ 2 Abs. 3 BDSG). Nicht-öffentliche Stellen sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie nicht unter § 2 Abs. 1-3 BDSG fallen. Soweit eine nicht-öffentliche Stelle aber hoheitliche Aufgaben der öffentlichen Verwaltung wahrnimmt, ist sie wiederum als öffentliche Stelle zu behandeln (§ 2 Abs. 4 BDSG).

Es besteht keine eindeutige Kompetenzzuweisung des Datenschutzes, sodass grds. die Länder zuständig sind (Art. 70 GG). Allerdings besteht eine Zuständigkeit kraft Sachzusammenhangs, soweit der Bund eine ihm zugewiesene Materie nicht ordnungsgemäß regeln kann, ohne datenschutzrechtliche Bestimmungen mit zu regeln.[17] Beispiele hierfür sind die Telekommunikationsnetze, Bundesbehörden oder auch allgemein privatrechtliche Unternehmen, da dem Bund die Zuständigkeit für Wirtschaft zufällt.[18]

Da alle Bundesländer von der Möglichkeit des Erlasses eigener Datenschutzgesetze Gebrauch gemacht haben, sind im Rahmen der Länderzuständigkeit die Landesdatenschutzgesetze anzuwenden. Das Landesdatenschutzgesetz welchen Landes anzuwenden ist, ergibt sich aus der örtlichen Zuständigkeit der Länder als Gebietskörperschaften (nur) für ihr eigenes Hoheitsgebiet.

[16] Vgl. § 1 Abs. 2 Nr. 2 BDSG, wonach das BDSG nur – und dann auch nur eingeschränkt – in den Ländern gelten würde, wenn kein Landesgesetz den Datenschutz regeln würde.
[17] BeckOK/*Wagner/Brink*, Datenschutzrecht, Syst. D, Rn. 57.
[18] Simitis/*Simitis*, BDSG, § 1 Rn. 6.

Das Schleswig-Holsteinische Gesetz zum Schutz personenbezogener Informationen (LDSG S-H) spricht insoweit von der „datenverarbeitenden Stelle“ und definiert diese als „jede öffentliche Stelle im Sinne von § 3 Abs. 1, die personenbezogene Daten für sich selbst verarbeitet oder durch andere verarbeiten lässt“ (§ 2 Abs. 3 LDSG S-H). Räumlich ist das LDSG S-H für Stellen mit Sitz in Schleswig-Holstein anzuwenden.

2. UKSH – Anstalt öffentlichen Rechts in Schleswig Holstein

Die Rechtmäßigkeit der Datenverarbeitung von Mitarbeiterdaten des Universitätsklinikums Schleswig Holstein (UKSH) im Rahmen von ITS.APT anhand des LDSG S-H zu beurteilen. Das UKSH ist eine rechtsfähige Anstalt des öffentlichen Rechts der Christian-Albrechts-Universität zu Kiel und der Universität zu Lübeck.[19] Damit ist es eine öffentlich-rechtlich organisierte Einrichtung des Landes Schleswig-Holstein i.S.d. § 2 Abs. 2 S. 1 Var. 3 BDSG, bzw. § 3 Abs. 1 S. 2 Var. 2 LDSG S-H i.V.m. § 41 Abs. 1 Allgemeines Verwaltungsgesetz für das Land Schleswig-Holstein (LVwG S-H).

Allerdings ist das UKSH teilprivatisiert. Hinsichtlich der IT führte dies zur Gründung der UKSH Gesellschaft für Informationstechnologie mbH (GfIT) und der UKSH Gesellschaft für IT Services mbH (UKSH ITSG). Für die Koordination und Durchführung von IT-Projekten im UKSH, sowie strategische Entscheidungen die UKSH-interne IT betreffend ist die Stabsstelle Informationstechnologie zuständig.[20]

Für die beiden GmbHen – als privatrechtlich organisierte Gesellschaften – gilt das BDSG.

3. Datenschutzrechtliche Beziehung UKSH – GmbH(en)

Zwischen dem UKSH und der GfIT besteht ein sog. Auftragsdatenverarbeitungsverhältnis. Die Verarbeitung personenbezogener Daten im Auftrag ist in § 17 LDSG S-H geregelt. Kernelement des Auftragsdatenverarbeitungsverhältnisses ist die Weisungsgebundenheit des Auftragnehmenden. Personenbezogene Daten sind durch den Auftragnehmenden nur im Rahmen der Weisungen durch den Auftraggeber – die datenverarbeitende Stelle – zu verarbeiten. Hierfür hat die datenverarbeitende Stelle zu sorgen (§ 17 Abs. 3 S. 1 LDSG S-H). Dementsprechend bleibt die datenverarbeitende Stelle selbst für die Einhaltung der Vorschriften der Datenschutzbestimmungen und die Gewährleistung der Betroffenenrechte verantwortlich, auch wenn der eigentliche Umgang mit den Daten durch den Auftragnehmenden passiert (§ 17 Abs. 1 S. 1 LDSG S-H). In der Konsequenz gilt die

[19] http://www.uksh.de/Das+UKSH/Impressum.html
[20] http://www.uksh.de/Informationstechnologie/

Weitergabe von Daten zwischen datenverarbeitender Stelle und Auftragnehmenden nicht als Übermittlung (§ 17 Abs. 1 S. 3 LDSG S-H). Hinsichtlich der Vereinbarung und Unterhaltung eines rechtskonformen Auftragsdatenverarbeitungsverhältnisses gilt es diverse Vorgaben zu beachten, um die Weisungsgebundenheit (§ 17 Abs. 3 S. 1 LDSG S-H) des Auftragnehmenden praktisch umzusetzen: Die datenverarbeitende Stelle hat den Auftragnehmenden sorgfältig auszuwählen und zu überprüfen (§ 17 Abs. 3 S. 2, 3 LDSG S-H). Sowohl die Auftragserteilung selbst als auch ergänzende Weisungen sind schriftlich festzulegen (§ 17 Abs. 3 S. 4 LDSG S-H). Es empfiehlt sich, auch die Ergebnisse der jederzeit durch den Auftragnehmenden zu ermöglichenden Kontrollen schriftlich festzuhalten.[21]

Im Zusammenhang mit der Verarbeitung von Gesundheitsdaten stellt sich die Frage nach der generellen Zulässigkeit von Auftragsdatenverarbeitung. Gem. § 1 Abs. 3 BDSG lassen die Normen des BDSG die „Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnisse, die nicht auf gesetzlichen Vorschriften beruhen“ unberührt. Auch das LDSG S-H stellt in § 3 Abs. 3 klar, dass besondere Rechtsvorschriften, die den Umgang mit personenbezogenen Daten regeln, vorgehen.

Grds. folgt daraus zunächst, dass die berufsrechtliche ärztliche Schweigepflicht[22] auch im Verhältnis zu eventuellen Auftragsdatenverarbeitern gilt. Entsprechend fordert die Bundesärztekammer ergänzend zur Einhaltung der Vorgaben in § 11 BDSG, dass technisch ausgeschlossen wird, dass ein „externer Dienstleister Kenntnis von den personenbezogenen Patientendaten nehmen kann“.[23] Hinsichtlich der Zulässigkeit von Auftragsdatenverarbeitung von Sozialdaten existieren diverse spezialgesetzliche Regelungen, etwa in den Sozialgesetzbüchern (SGB).[24] Die Regelungen nach SGB sind jedoch nur für die Datenverarbeitung bei Sozialleistungsträgern anzuwenden, konkret also nicht beim UKSH sondern bei den öffentlichen Kranken-, Pflege- Renten oder Unfallkassen. Im Rahmen des Projekts spielen diese Datenkategorien bzw. -nutzungen daher keine Rolle.

Eine formale oder inhaltliche Prüfung des zwischen dem UKSH und der GfIT bestehenden Auftragsdatenverarbeitungsverhältnisses ist im Rahmen des Projektes nicht vorgesehen und

[21] Vgl. die entsprechende Regelung in § 11 Abs. 2 S. 5 BDSG.
[22] § 9 MBO-Ä; Stand Juli 2015, http://www.bundesaerztekammer.de/fileadmin/user_upload/downloads/pdf-Ordner/MBO/MBO_02.07.2015.pdf. Zur Strafbewährtheit der Offenbarung von Geheimnissen und den hieraus folgenden Konsequenzen für die Projektdurchführung vgl. sogleich unter IV.
[23] http://www.bundesaerztekammer.de/fileadmin/user_upload/downloads/Schweigepflicht_2014.pdf, S. A 969.
[24] Vgl. etwa Weichert, „Stellungnahme zum Entwurf eines Gesetzes zur Änderung krankenversicherungsrechtlicher und anderer Vorschriften (BT-Drs. 17/1297) insbesondere zur Frage der Einschaltung Privater bei Abrechnungen im Rahmen der gesetzlichen Krankenversicherung“, https://www.datenschutzzentrum.de/medizin/gkv/20100519-stellungnahme-hzv.html

auch nicht erforderlich. Das UKSH hat sich vertraglich entsprechende Weisungsrechte vorbehalten sowie einen dem § 17 LDSG entsprechenden Vertrag geschlossen.

4. Exkurs: Die Europäische Datenschutz-Grundverordnung

Die europäische Datenschutz-Grundverordnung (DS-GVO)[25] wird nach ihrer Annahme durch das Europäische Parlament und den Europäischen Rat mit einer Übergangsfrist von zwei Jahren das deutsche BDSG und die LDSGe „ablösen". Nach ihrem Inkrafttreten wird die DS-GVO erst mit einer Übergangsfrist von zwei Jahren Anwendung finden. Während der Durchführung des Projektes ITS.APT wird die DS-GVO mithin für die Rechtslage nicht maßgeblich werden.

Sobald die DS-GVO anwendbar ist, besteht ein Anwendungsvorrang dieses europäischen Rechts gegenüber nationalem Recht; die nationalen Datenschutzvorschriften werden somit nicht außer Kraft gesetzt, sondern sie sind nur noch subsidiär anzuwenden: Da Anwendungsvorrang nicht auch Geltungsvorrang bedeutet, gelten alle nationalen Vorschriften weiter. Aber sie sind insoweit nicht anwendbar, als sie den Regelungen der DS-GVO (sowie eventueller delegierter Rechtsakte der Europäischen Kommission aufgrund entsprechender Ermächtigungen in der DS-GVO) widersprechen.[26] Eine nationale Regelung wird auch unanwendbar, wenn sie nur „indirekt" einer Regelung der DS-GVO widerspricht, d.h. wenn die Normen eigentlich verschiedene Sachverhalte regeln, dabei aber sich widersprechende Ergebnisse liefern. In diesen Fällen darf die nationale Regelung es nicht praktisch unmöglich machen oder übermäßig erschweren, durch Unionsrecht verliehene Rechtspositionen auszuüben (Effektivitätsgrundsatz).[27]

Über das zuvor Gesagte hinaus, wird den Mitgliedstaaten durch einige sog. „Öffnungsklauseln" in der DS-GVO die Möglichkeit eingeräumt, jeweils genauere bereichsspezifische Regelungen zu treffen. Gemeint sind Vorschriften, die die Ausgestaltung oder Beschränkung des Regelungsinhalts den Mitgliedstaaten überlassen.

Dies gilt z.B. für den Bereich des Beschäftigtendatenschutzes (Art. 88 DS-GVO), der für ITS.APT von hoher praktischer Relevanz ist (vgl. hierzu Dokument 2.1 „Arbeitsrechtliche Betrachtung").

[25] http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CONSIL:ST_5419_2016_INIT&from=DE
[26] Maunz/Dürig/*Giegerich*, GG, Art. 123 Rn. 61.
[27] EuGH C 231/96 – Edis, Rn. 34.
http://curia.europa.eu/juris/document/document.jsf?text=&docid=44055&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1

D. Datenschutzrechtliche Grundlagen für Testdurchführung

In Anbetracht dessen, dass die Testdurchführung im realen „Normalbetrieb“ des UKSH erfolgen soll, sind zunächst die sich speziell aus dem Testumfeld ergebenden datenschutzrechtlichen Rahmenbedingungen genau zu prüfen. Die anvisierten Maßnahmen müssen sich im Rahmen des rechtlich Zulässigen bewegen. Der Schutz der Daten der Mitarbeiter als „Probanden“ ist dabei genauso relevant wie der Schutz der Daten der Patienten des UKSH.

I. Einbringen des Programms in die UKSH-IT

Automatisierte Verfahren zur Datenverarbeitung sind vor ihrem erstmaligen Einsatz und nach wesentlichen Änderungen hinsichtlich einer wirksamen Umsetzung der zur Datensicherheit vorzunehmenden Maßnahmen zu testen und freizugeben (§ 5 Abs. 2 LDSG S-H). Näheres hierzu regelt gem. § 5 Abs. 3 LDSG S-H eine Rechtsverordnung. Auf dieser Grundlage wurde die schleswig-holsteinische Landesverordnung über die Sicherheit und Ordnungsmäßigkeit automatisierter Verarbeitung personenbezogener Daten (Datenschutzverordnung – DSVO S-H) erlassen, die die Dokumentation automatisierter Verfahren bei der Verarbeitung personenbezogener Daten durch öffentliche Stellen sowie deren Tests und Freigabe dieser Verfahren (§ 1 Abs. 1 DSVO S-H) regelt.

Ihre Bestimmungen sind für ITS.APT relevant, da – wie bereits ausgeführt – zur Testdurchführung ein durch das Projekt entwickeltes Programm in die IT des UKSH eingebracht werden muss. Automatisierte Verfahren i.S.d. der DSVO S-H sind „Arbeitsabläufe mit Hilfe von informationstechnischen Geräten, Programmen und automatisierten Dateien“ (§ 2 Nr. 1 DSVO S-H), wobei „informationstechnische Geräte“ die benötigte Hardware – Server, Router, Arbeitsplatzrechner etc. – meint (§ 2 Nr. 2 DSVO S-H) und „Programme“ die Software (§ 2 Nr. 3 DSVO S-H). Soweit am UKSH also rechnergestützt gearbeitet wird, E-Mails versandt und empfangen, sowie bspw. Patientenakten digital am Rechner gepflegt werden, handelt es sich um automatisierte Verfahren, die gem. § 3 DSVO S-H zu dokumentieren sind.

Auch bei dem von ITS.APT zu entwickelnden Testtool handelt es sich um ein Programm in diesem Sinn, das zu Datenerhebung und weiterer –verarbeitung in einem automatisierten Verfahren führt. Dementsprechend ist es gem. § 5 Abs. 1 S. 1 DSVO S-H vor Aufnahme der Verarbeitung personenbezogener Daten – in diesem Falle: vor seinem erstmaligen Einsatz – zu testen und die Testmaßnahmen, sowie erzielten Ergebnisse sind zu dokumentieren (§ 5 S. 2 DSVO S-H). Soweit keine wesentlichen Mängel festgestellt werden, kann sodann die –

zwingend schriftliche – Freigabe erfolgen (§ 5 Abs. 2 DSVO S-H). Die Freigabe kann gem. § 5 Abs. 2 LDSG S-H durch die Leitung der datenverarbeitenden Stelle oder eine befugte Person vorgenommen werden..

II. Medizinische Daten

Neben speziellen berufsrechtlichen Normen, ist die Verletzung der ärztlichen Schweigepflicht auch allgemein strafbewährt. § 203 StGB stellt die Verletzung von Privatgeheimnissen unter Strafe. Wer unbefugt ein fremdes Geheimnis offenbart, das ihm als Arzt, Apotheker oder Angehöriger eines anderen Heilberufs anvertraut worden oder sonst bekannt geworden ist, macht sich gem. § 203 Abs. 1 Nr. 1 StGB strafbar. Zu letzteren gehören u.a. Krankenschwestern und –pfleger, Kinderkrankenschwerstern und –pfleger, sowie Krankenpflegehelferinnen und –helfer.[28] Gleiches gilt für deren berufsmäßig tätige Gehilfen und die Personen, die bei ihnen zur Vorbereitung auf den Beruf tätig sind (§ 203 Abs. 3 S. 2 StGB). Das technische Wartungs- und Bedienungspersonal ist von der Strafnorm grds. erfasst, vorausgesetzt es ist fest in die Organisation eingebunden.[29] Da die UKSH GfIT, bzw. ihre Beschäftigten, ausschließlich informationstechnische Leistungen für das UKSH erbringt, könnte diese Voraussetzung hier erfüllt sein. Allerdings wird die Regelung nicht auf Auftragsdatenverarbeiter wie die IT-GmbHen angewendet, da es bei ihnen an einer hinreichenden arbeitsrechtlichen Weisungsgebundenheit fehlt. Soweit als die IT-GmbHen mit dem § 203 StGB unterfallenden medizinischen Daten umgehen, basiert dies auf Grundlage von Einwilligungen der Patienten.[30] Diese Einwilligungen umfassen jedoch nicht die Projektdurchführung durch ITS.APT.

Die Norm dient dem Schutz des verfassungsmäßig gewährleisteten allgemeinen Persönlichkeitsrechts der Betroffenen, sowie dem des Rechts auf informationelle Selbstbestimmung, d.h. die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.[31] „Offenbaren“ ist jede Mitteilung über die geheim zu haltende Tatsache an einen Dritten. Umfasst ist auch die Identität der Person, um deren Geheimnis es sich handelt.[32] Das bedeutet, dass bereits die Tatsache, dass eine Person in einem Behandlungsverhältnis zu einem Arzt steht, geheim ist. Soweit es um strafrechtlich relevante Inhalte geht, die digital gespeichert sind, genügt die Einräumung der

[28] Lackner/Kühl/*Heger*, StGB, § 203 Rn. 3.
[29] Lackner/Kühl/Heger, StGB, § 203 Rn. 11b.
[30] Vgl. Orientierungshilfe Krankenhausinformationssysteme, Szenarienkatalog, http://datenschutzzentrum.de/medizin/krankenh/OH_KIS.pdf, S. 2.
[31] BVerfG, Beschluss vom 14. Dezember 2001 – Az.: 2 BvR 152/01, Rn. 19.
[32] Lackner/Kühl/Heger, StGB, § 203 Rn. 17.

Verfügungsgewalt über die Daten, d.h., Weitergabe des Datenträgers oder der Datei.[33] Zugriff Externer auf die IT-Systeme, mit denen Patientendaten verarbeitet werden, kann den Tatbestand mithin erfüllen. Bereits wenn die Möglichkeit der inhaltlichen Kenntnisnahme eingeräumt wird, z.B. durch Unterlassen gebotener Sicherungsmaßnahmen in Garantenstellung, ist der Tatbestand vollendet.[34] Im Kontext von ITS.APT bedeutet dies, dass die Projektmitarbeiter – mit Ausnahme der am UKSH beschäftigten und in die Organisation eng eingebundenen Personen – nicht unmittelbaren Zugriff auf die IT-Infrastruktur des UKSH bzw. der UKSH GfIT erhalten dürfen. Andernfalls würden sich beteiligte Beschäftigte des UKSH und/oder der IT-Tochtergesellschaft(en) ggf. dem Risiko der Strafverfolgung aussetzen, was in jedem Falle vermieden werden soll.

III. Erhebung

§ 2 Abs. Nr. 1 LDSG S-H definiert das Erheben als „Beschaffen von Daten“. Dies entspricht inhaltlich der Definition des BDSG,[35] sodass hier auf die entsprechende Kommentierung zurückgegriffen werden kann. Die datenverarbeitende Stelle muss sich auf irgendeine Art und Weise die Daten willentlich beschafft haben. Dies ist für die Reaktion der Mitarbeiter auf die vorgespiegelten Sicherheitsrisiken in Rahmen des Testversuchs der Fall. Das UKSH erhebt diese Informationen. Auch im Falle der Mitteilung durch eine andere Stelle liegt für die erhaltende Stelle eine Erhebung vor. Allerdings muss die Stelle die Daten gezielt für einen Zweck entgegennehmen; nur die Mitteilung führt noch nicht zu einer Erhebung im Rechtssinne.[36]

1. §§ 11 Abs. 1 Nr. 2, 13 Abs. 1 LDSG S-H

§§ 11 Abs. 1 Nr. 2, 13 Abs. 1 LDSG S-H bzw. gestattet die Erhebung von personenbezogenen Daten aufgrund einer „anderen Rechtsvorschrift“. Eine solche kann auch eine Betriebs- oder Dienstvereinbarung sein.[37] Im Rahmen des Projektes wird angestrebt, eine solche zwischen UKSH und dem (Gesamt-)Personalrat des UKSH zu schließen, um eine Erhebungsgrundlage zu schaffen.

Eine Dienstvereinbarung muss den Vorgaben des § 32 BDSG genügen.[38] Es gelten alle allgemeinen gesetzlichen Anforderungen vom Grundsatz der Datensparsamkeit, über den

[33] Schönke/Schröder/*Eisele/Lenckner*, StGB, § 203 Rn. 19.
[34] Lackner/Kühl/*Heger*, StGB, § 203 Rn. 17.
[35] § 3 Abs. 3 BDSG
[36] Däubler/Klebe/Wedde/Weichert/*Weichert*, BDSG, § 3 Rn. 31.
[37] Vgl. hierzu Dokument 2.1, S. 21 ff.
[38] Vgl. hierzu Dokument 2.1, S. 23.

Grundsatz der Direkterhebung und organisatorisch-technische Maßnahmen bis zu den Betroffenenrechten.[39]

2. § 22 LDSG S-H

§ 22 LDSG S-H gestattet die Verarbeitung personenbezogener Daten zu wissenschaftlichen Zwecken. „Datenverarbeitung" umfasst begrifflich das Erheben, Speichern, Übermitteln, Sperren, Löschen, Anonymisieren und Pseudonymisieren personenbezogener Daten (§ 2 Abs. 2 LDSG S-H), sodass – anders als nach § 40 BDSG[40] – die Datenerhebung zu wissenschaftlichen Zwecken an gleicher Stelle geregelt ist wie auch die übrige (Weiter-)Verarbeitung.

Die Wissenschaft steht unter dem besonderen Schutz des Grundgesetzes. Art. 5 Abs. 3 S. 1 GG bestimmt, dass sie „frei" ist. Als sog. „prinzipiell schrankenloses Grundrecht"[41] genießt die Wissenschaftsfreiheit das Privileg, nur durch andere verfassungsrechtlich geschützte Rechtsgütern eingeschränkt werden zu können.[42] Kollisionen müssen insoweit „nach Maßgabe der grundgesetzlichen Wertordnung und unter Berücksichtigung der Einheit dieses Wertsystems durch Verfassungsauslegung gelöst werden".[43] Im Wege der praktischen Konkordanz muss eine Gesamtabwägung am Maßstab des Verhältnismäßigkeitsprinzips erfolgen, mit dem Ziel, die kollidierenden Rechtsgüter in einen angemessenen Ausgleich zu bringen.[44] Im Rahmen des Datenschutzrechtes kommt als konkurrierendes Grundrecht hier insbesondere das Recht auf informationelle Selbstbestimmung derjenigen in Betracht, deren personenbezogene Daten Gegenstand der wissenschaftlichen Betrachtung werden (sollen). Das bedeutet, dass zu wissenschaftlichen Zwecken zwar umfänglich personenbezogene Daten verarbeitet werden sollen und dürfen, jedoch die Betroffenen nicht völlig schutzlos gestellt sind in Anbetracht des „guten Zwecks" der Wissenschaft. Diese Abwägung spiegeln sowohl § 40 BDSG, als auch § 22 LDSG S-H wider, u.a. indem sie vergleichsweise weite Erlaubnistatbestände bieten, allerdings gleichzeitig eine strenge, bzw. absolute Zweckbindung von zu Forschungszwecken erhobenen Daten kodifizieren.[45]

---

[39] *Wybitul*, NZA 2014, 225 (231).
[40] § 40 BDSG beschränkt sich auf die Regelung der Verwendung bereits zu wissenschaftlichen Zwecken erhobener und/oder gespeicherter Daten für wissenschaftliche Zwecke; Simitis/*Simitis*, BDSG, § 40 Rn. 1. Vgl. auch bereits Dokument 2.1 „Arbeitsrechtliche Betrachtung".
[41] Maunz/Dürig/*Scholz*, GG, Art. 5 Abs. 3 Rn. 14.
[42] Beck'scher Online-Kommentar GG/*Kempen*, Art. 5 Rn. 199.
[43] BVerfG, Beschluss vom 01. 03. 1978 – Az.: 1 BvR 174, 178, 191/71; 333/75, Rn. 154.
[44] BVerfG, Beschluss vom 27.11.1990 – Az.: 1 BvR 402/87, Rn. 40, 54, 56.
[45] Vgl. Weichert, Beitrag für die Deutsche Zeitschrift für Klinische Forschung – Aktuelle Herausforderungen des Datenschutzes im Bereich der medizinischen Forschung, III; online verfügbar: https://www.datenschutzzentrum.de/artikel/147-Medizinische-Forschung-Herausforderungen-des-Datenschutzes.html#extended.

Voraussetzung der Anwendbarkeit des §§ 22 LDSG S-H ist, dass die Datenerhebung zu wissenschaftlichen Zwecken erfolgt. Der Wissenschaftsbegriff ist weit auszulegen: Erfasst sind nicht nur bestimmte wissenschaftliche Auffassungen oder Theorien sondern auch Mindermeinungen, Forschungsansätze und -ergebnisse, die sich im Nachhinein als „irrig oder fehlerhaft“ erweisen, sowie „unorthodoxes oder intuitives Vorgehen“. Der Schutz nur einer bestimmten Auffassung wäre unvereinbar mit der der Wissenschaft eigenen „prinzipiellen Unvollständigkeit und Unabgeschlossenheit“.[46] Andererseits gilt ein Werk nicht schon als „wissenschaftlich“, weil der Urheber es so bezeichnet.[47] Vorausgesetzt werden allgemein Erkenntnisgewinnung durch die Gewährleistung äußerer Autonomie, d.h. Freiheit vor Einflussnahmen durch Dritte, sowie ein planmäßiges Vorgehens nach einer bestimmten, nachvollziehbaren Methode, sodass die Ergebnisse einer kritischen Prüfung zugänglich sind.[48]

Dies ist bei dem hier zu beurteilenden Projektvorhaben der Fall. Es werden systematische Ansätze verfolgt, das IT-Sicherheitsbewusstsein von Beschäftigten nicht nur zu testen, sondern dann auch möglichst zu erhöhen. Dies erfolgt in zwei Testrunden, insbesondere um eine Verifikation der Ergebnisse zu ermöglichen. Zudem wird das Vorgehen dokumentiert und veröffentlicht und so zum wissenschaftlichen Diskurs beigetragen. Schließlich wird die Maßnahme vorgenommen durch Einrichtungen, die sich der wissenschaftlichen Forschung verschrieben haben und als weiteres Indiz wird das Gesamtvorhaben im Rahmen der Forschungsförderung durch das Bundesministerium für Bildung und Forschung (BMBF) finanziert.

Weitere Voraussetzungen des „Forschungsparagraphen“ § 22 LDSG sind, dass die Daten durch eine öffentliche Stelle anonymisiert oder pseudonymisiert verarbeitet werden. Das UKSH als öffentliche Stelle – könnte zu Forschungszwecken die für ITS.APT erforderlichen Daten erheben. Allerdings kommt vorliegend weder eine anonyme, noch eine pseudonyme Erhebung in Betracht: Eine anonyme Erhebung wäre zwar technisch möglich, würde aber den Forschungszweck nicht erfüllen, da sodann z.B. keine Erhebung weiterer Personaldaten und deren Zuordnung zu den Testergebnissen erfolgen könnten. Eine pseudonyme Erhebung ist denklogisch nur möglich, wenn die „Erhebung“ („das Beschaffen von Daten“, § 2 Abs. 2 Nr. 1 LDSG S-H) bei der maßgeblichen öffentlichen Stelle durch die Übermittlung der Daten von dritter Seite geschieht. Dann könnte die Zuordnungsfunktion bei der übermittelnden Stelle verbleiben, sodass die Daten aus Sicht der empfangenden Stelle pseudonym erhoben

[46] BVerfG, Beschluss vom 11.01.1994 – Az.: 1 BvR 434/87, Rn. 49.
[47] BVerfG, Beschluss vom 11.01.1994 – Az.: 1 BvR 434/87, Rn. 50.
[48] Beck’scher Online-Kommentar/*Kempen*, GG, Art. 5 Rn. 181.

werden. Das ist in der in ITS.APT gegebenen Konstellation nicht möglich, da das UKSH die Daten originär erheben wird und die Zuordnungsfunktion im Haus vorhanden ist. Um den Erfordernissen einer möglichst sicheren Verarbeitung von Forschungsdaten gerecht zu werden, werden die Daten dennoch zeitnah getrennt. Die Identitäten der Mitarbeiter werden dabei nicht unmittelbar zusammen mit den Angaben zu den jeweiligen Reaktionen gespeichert. Die Zuordnungstabelle wird gesondert gespeichert. Rückgriffe darauf erfolgen und nur soweit erforderlich, z.B. zur individualisierten erneuten Kontrolle nach Abschluss der Schulung, Vergleich des Erfolges der Weiterbildung durch Abgleich der Reaktionen vor und nach der Schulung.

§ 22 Abs. 3 LDSG S-H eröffnet für den Fall, dass weder eine anonyme, noch eine pseudonyme Verarbeitung – hier: Erhebung – möglich ist, weitere Möglichkeiten. Eine Datenerhebung zu wissenschaftlichen Zwecken wäre hiernach auch möglich mit der Einwilligung der Betroffenen (Nr. 1), soweit es sich nicht um Daten der besonderen Kategorien (§ 11 Abs. 3 LDSG S-H) handelt wenn schutzwürdige Belange der Betroffenen wegen der Art der Daten oder wegen der Art der Verwendung für das jeweilige Forschungsvorhaben nicht beeinträchtigt sind (Nr. 2) oder wenn die die Genehmigung der für die datenverarbeitende Stelle zuständigen obersten Aufsichtsbehörde vorliegt (Nr. 3).

§ 23 LDSG S-H

§ 23 LDSG S-H ist die landesgesetzliche Erhebungsgrundlage für personenbezogene Daten im Dienst- und Arbeitsverhältnis. Insofern kann auf die vertieften Ausführungen in Dokument 2.1 – Arbeitsrechtliche Betrachtung verwiesen werden.

IV. Weitere Verarbeitung

Nach Erhebung der Daten wird das UKSH die pseudonymisierten Daten einzelnen Projektpartnern zur Verfügung stellen, um ihnen die (Weiter-)Verarbeitung der Daten entsprechend ihrer jeweiligen Teilvorhaben im Projekt zu ermöglichen. Hierbei handelt es sich um eine Übermittlung: Übermitteln ist das Weitergeben von Daten an Dritte oder der Abruf von zum Abruf bereitgehaltenen Daten durch Dritte (§ 2 Abs. 2 Nr. 3 LDSG S-H). Die Projektpartner sind „Dritte“ im Sinne der Norm, da sie organisatorisch außerhalb der speichernden Stelle UKSH stehen.[49]

[49] Vgl. zur inhaltlich identischen Definition in § 3 Abs. 2 Nr. 3 BDSG: Däubler/Klebe/Wedde/Weichert/*Weichert*, BDSG, § 3 Rn. 39.

1. Rechtliche Anforderungen

Nach § 22 Abs. 7 LDSG S-H ist die Übermittlung an empfangende Stellen, auf die das LDSG S-H keine Anwendung findet, nur unter weiteren Voraussetzungen gestattet: Die empfangenden Stellen sind zu verpflichten die Vorschriften § 22 Abs. 5 und Abs. 6 LDSG S-H einzuhalten. Nach Abs. 5 sind die Daten zu anonymisieren bzw. pseudonymisieren sobald der Forschungszweck es gestattet. Die Weiterverarbeitung für andere Zwecke ist zulässig, soweit die Voraussetzungen der § 22 Abs. 1 bis 3 LDSG S-H erfüllt werden. Das bedeutet, eine „Umwidmung" von Forschungsdaten zu forschungsfremden Zwecken ist nicht möglich.

Hinsichtlich eventueller Veröffentlichungen bestimmt Abs. 6, dass eine Veröffentlichung personenbezogener Daten nur mit Einwilligung der Betroffenen (Nr. 1), oder wenn die Darstellung von Forschungsergebnissen über Personen der Zeitgeschichte unerlässlich ist (Nr. 2), zulässig ist. Die Veröffentlichung etwa von anonymisierten oder aggregierten Angaben wie statistischen Werten stellt dabei i.d.R. kein Problem dar, da hier der Personenbezug nicht (wieder)herstellbar ist.

Während für die Erhebung der personenbezogenen Daten im Rahmen von ITS.APT der Abschluss einer Dienstvereinbarung essentiell ist (vgl. bereits D. III.), kann die weitere Verarbeitung – zu Forschungszwecken – direkt auf die Erlaubnis in § 22 LDSG S-H gestützt werden. Die Anforderungen an eine die Dienstvereinbarung werden ausführlich in Dokument 2.1 (siehe dort Kapitel E. und F.)erörtert.

2. Technische Anforderungen

Wie bereits mehrfach angesprochen, spielt im Kontext einer datenschutzrechtlichen Analyse des ITS.APT-Projektszenarios der Begriff der Anonymität – und dazu abgegrenzt der Begriff der Pseudonymität – eine wichtige Rolle. So unterfällt ist die Verarbeitung anonymisierter Daten nicht den Einschränkungen des Datenschutzrechts, wogegen lediglich pseudonymisierte Daten sehr wohl datenschutzrechtlichen Bestimmungen unterliegen. Die Problematik hierbei besteht unter Anderem in der klaren Trennung dieser beiden Begrifflichkeiten in der Anwendungspraxis.

Zum Begriff der Anonymisierung als dem Vorgang der Überführung personenbezogener oder personenbeziehbarer Daten in eine anonymisierte Form führt § 2 Nr. 6LDSG aus:

„Anonymisieren das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem

unverhältnismäßigen Aufwand einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können,"

Dabei werden zwei Varianten der Anonymisierung beschrieben: die echte Anonymisierung, bei der die Daten nach dem Vorgang gar keinen Personenbezug mehr aufweisen (statistische Datensätze nach Löschen der personenbezogenen Teile der Erhebungsbögen) und die faktische Anonymisierung bei der in den Datensätzen Informationen verblieben, die zumindest theoretische eine Deanonymisierung ermöglichen.[50] Welche Anforderungen an einen unverhältnismäßigen Aufwand zu stellen sind ist unter Berücksichtigung von Art und Umfang der zu schützenden Daten zu bestimmen.[51]

Die Bestimmungen des BDSG sind inhaltlich vergleichbar:

„Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können." [52]

Parallel hierzu wird der Vorgang der Pseudonymisierung definiert:

„Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren."[53]

Für die datenschutzrechtliche Analyse der Projektgegenstände im Projekt ITS.APT ergibt sich entsprechend ein Bedarf, die hier vorliegenden Datenbestände und zugehörigen Datenverarbeitungsvorgänge hinsichtlich ihres entsprechenden Charakters zu bewerten. Handelt es sich bei den zu verarbeitenden Daten um (hinreichend) anonymisierte Daten, fallen sie nicht unter das BDSG. Handelt es sich jedoch um nicht hinreichend anonymisierte Daten, so ist ein Rückschluss auf die Identität Betroffener (ohne hinreichend großen Aufwand) möglich. Insoweit handelt es sich folglich nicht mehr um anonymisierte, sondern bestenfalls um pseudonymisierte Daten. Daher ist eine Unterscheidung ob dieses Charakters essentiell notwendig.

Der Vorgang der Anonymisierung beschreibt den Ansatz, personenbezogene oder personenbeziehbare Daten derart abzuändern, dass ein Personenbezug nicht mehr

[50] ULD, Hinweise zur Anwendung des Schleswig-Holsteinischen Gesetzes zum Schutz personenbezogener Informationen, 2002, https://www.datenschutzzentrum.de/download/hinwldsg.pdf, § 2 Ziff. 21.
[51] ULD, a.a.O., § 2 Ziff. 21.
[52] §3 Abs. 6 BDSG.
[53] §3 Abs. 6a BDSG.

rekonstruiert werden kann. Dies kann generell durch verschiedene technische Verfahren erreicht werden, von denen die wichtigsten nachfolgend kurz erläutert werden.

a. Anonymisierung durch Löschung

Bei diesem Verfahren werden gezielt personenidentifizierende Daten aus Datensätzen herausgelöscht, um den Personenbezug aufzuheben. Führt eine Tabelle etwa eine Liste mit den Merkmalen NAME und GEBURTSJAHR, so ist klar ein hinreichend identifizierender Personenbezug ableitbar. Eine Anonymisierung durch Löschung könnte nun darin bestehen, die Spalte NAME vollständig zu löschen. Die verbleibenden Datensätze enthielten folglich nur noch die Geburtsjahre, die sich zunächst nicht ohne weiteren Aufwand einer natürlichen Person zuordnen lassen.

Die Schwachstelle dieses Verfahrens besteht in der Verkettbarkeit der verbliebenen Daten mit externen Informationsquellen. Handelt es sich bei den Datensätzen der Tabelle beispielsweise um Mitarbeiter in einem kleinen Unternehmen, so lassen sich die Datensätze mancher Mitarbeiter, etwa des Paktikanten oder der Rentenanwärterin, sehr leicht auch allein aus den Geburtsjahren re-identifizieren. Hier kann folglich definitiv nicht von einem hinreichend großen Aufwand zur Re-Identifizierung natürlicher Personen gesprochen werden, da anzunehmen ist, dass jeder Mitarbeiter des Unternehmens über derartiges Kontextwissen verfügt. Folglich liegt hier zwar der Versuch einer Anonymisierung vor, es findet aber keine hinreichende Anonymisierung statt. Ein entsprechendes Risiko für eine Re-Identifizierung bergen auch alle sonstigen Informationen in der Datenbank, die sich zu einer konkreten Person beziehen lassen (z.B.: Zeitstempel)

b. Anonymisierung durch Generalisierung

Bei diesem Verfahren werden Daten derart verändert, dass ihr Informationsgehalt insgesamt reduziert wird – ohne die eigentliche Datensemantik zu ändern. Als Beispiel könnte obiger Datensatz aus Geburtsjahren derart verändert werden, dass anstelle des exakten Geburtsjahres nur noch das Jahrzehnt der Geburt erhalten bleibt; die letzte Ziffer des Geburtsjahres würde quasi gelöscht. Ähnliche Verfahren gibt es auch für andere Datentypen, etwa bei Berufsgruppen (z.B. Bäcker < Handwerker < Selbständige < KMU) oder Herkunftsdaten (z.B. Stadt < Region < Nationalität < Kontinent).

Analog zur Anonymisierung durch Löschung ergeben sich hier durch zusätzliches Kontextwissen Möglichkeiten zur Re-Identifizierung einzelnen Individuen. So mag selbst das Geburtsjahrzehnt ausreichend sein, um den Praktikanten von der Stammbelegschaft eines Unternehmens zu unterscheiden.

c. *Anonymisierung durch Perturbation*

Bei diesem Verfahren werden Datensätze miteinander verschnitten oder zusätzliche Daten hinzugefügt, um originäre Bezüge innerhalb der Daten zu verschleiern. So können beispielsweise weitere Datensätze zu einer bestehenden Tabelle hinzugefügt werden, um gezielten Re-Identifizierungangriffen entgegenzuwirken. In obigem Beispiel würden also weitere Geburtsjahrzehnte dem Datensatz hinzugefügt, um die besonderen, re-identifizierbaren Einzelfälle zu kaschieren. In der Folge würde der Datensatz schwerer zu De-Anonymisieren sein, was aber auch spürbare Auswirkungen auf die Verwendbarkeit der anonymisierten Daten mit sich brächte.

Bei der Anonymisierung durch Perturbation kann jeder vorhersehbaren Re-Identifizierungsattacke durch gezieltes Hinzufügen entsprechender Störinformationen entgegengewirkt werden. Kritisch zu betrachten sind hierbei jedoch zum einen die unvorhergesehenen Re-Identifizierungsmöglichkeiten, für die folglich auch keine entsprechende Fehlereinstreuung erfolgt ist, sowie zum anderen die Nutzbarkeit und Aussagekraft der anonymisierten – und daher verfälschten – Daten insgesamt.

d. *Anonymisierung durch Aggregation*

Bei dieser Methode werden mehrere bis alle Datensätze des zu anonymisierenden Datenbestandes miteinander verschmolzen, um Aussagen genereller Natur zu erhalten. Ähnlich der Anonymisierung durch Generalisierung geht hierbei die präzise Einzelinformation verloren zugunsten einer anonymeren, höherschwelligen Aussage. Ein Beispiel bestünde in der Berechnung des durchschnittlichen Geburtsjahres aller Mitarbeiter des besagten Unternehmens. Hierzu würde die Summe aller Geburtsjahre durch die Anzahl der Mitarbeiter geteilt; das Ergebnis hätte Aussagekraft zum Alter der Belegschaft, ließe aber keinen direkten Rückkanal zur Bestimmung des Alters einzelner Mitarbeiter zu – es sei denn, die Geburtsjahre sämtlicher anderen Mitarbeiter wären aus anderen Quellen bestimmbar.

Die Anonymisierung durch Aggregation kann nach heutigem Wissensstand als die sicherste Methode der Anonymisierung – nach der Anonymisierung durch Löschung – gesehen werden, da sie bei hinreichend großer Datenmenge gute bis sehr gute Anonymisierungsqualitäten erlaubt. Eine Re-Identifikation ist nur unter ungünstigen Umständen und bei kleineren Datenmengen realistisch, wobei dennoch die Gefahr besteht, dass eine solche Anonymisierung durch zusätzliche Kontextinformationen deutlich erleichtert wird. Verlässt etwa der Praktikant das Unternehmen, kann die Veränderung des durchschnittlichen Geburtsjahres Rückschlüsse auf das Alter des Praktikanten erlauben, was

ein personenbezogener Erkenntnisgewinn aus eigentlich anonymisierten Daten wäre, und damit die angenommene Anonymität der Daten falsifiziert.

e. K-Anonymität

Im forschungsseitigen Sprachjargon haben sich ausgehend von obigen Betrachtungen einige Begrifflichkeiten zu Anforderungen an eine hinreichende Anonymisierung entwickelt, die hier von Relevanz sein dürften. Zunächst definierte Latanya Sweeney im Jahr 2002 in einen vielbeachteten Aufsatz den Begriff der sogenannten K-Anonymität[54]. Grundgedanke dieser Definition ist es, durch Spezifikation geeigneter Abfragebeschränkungen dafür zu sorgen, dass ein Datenverarbeiter stets Datenbestände mit speziellem Charakter erhält. Essentielle Vorschrift hierbei ist, dass ein Datenbestand stets mindestens *k* vom Verarbeiter ununterscheidbare Datensätze enthält, so dass er nicht in der Lage ist, Informationen über Gruppen mit weniger als *k* Datensätzen zu erlangen. Sollte eine derartige Anfrage an den k-anonymisierten Datenbestand erfolgen, so muss die Datenverarbeitungsmethodik die Verarbeitung derart einschränken, dass nur entweder mindestens k identische Datensätze verarbeitet werden, oder gar keine Datenpreisgabe erfolgt.

Als Konzept hat sich die K-Anonymität einen hohen Stellenwert in der Forschung erarbeitet, bei der Durchsetzung in Datenverarbeitungssystemen der realen Welt ergeben sich hier jedoch gravierende Problemstellungen. So kann etwa die Weitergabe eines k-anonymisierten Datensatzes nicht erfolgen, falls der Empfänger eine andersgeartete k-anonymisierte Version derselben Daten zur Verfügung hat. Eine Ausprägung dieses Umstandes findet sich bei der Beobachtung eines Datenbestandes über die Zeit, d.h. über Änderungen am Datenbestand hinweg. Ist etwa per K-Anonymität (k=2) sichergestellt, dass im verarbeiteten Datenbestand stets zwei Mitarbeiter dasselbe Geburtsjahr aufweisen, so kann diese Zuordnung sich ändern, wenn der Praktikant das Unternehmen verlässt. Entsprechend erfolgt nun eine andere k-Anonymisierung, mit anderen Geburtsjahren, die bei Kenntnis des genauen Anonymisierungsverfahrens Informationen über das Geburtsjahr des Praktikanten zulassen. Darüber hinaus gibt es technische Schwierigkeiten bei der K-Anonymisierung komplexer Datenbestände wie Fließtext in menschlicher Sprache oder bei Abbildungen. Hierfür wurden weiterführende Anonymisierungskonzepte wie L-Diversity[55] und T-

[54] L. Sweeney: k-anonymity: A model for protecting privacy. In: International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, Vol. 10, Issue 5, World Scientific, 2002, S. 557-570
[55] A. Machanavajjhalaet al.: l-diversity: Privacy beyond k-anonymity. In: ACM Transactions on Knowledge Discovery from Data (TKDD), Vol. 1, ACM, 2007

Closeness[56] definiert, die jedoch ihrerseits technisch komplexe Fragestellungen hinsichtlich ihrer Realisierbarkeit aufwerfen.

f. Pseudonymisierung

Anders als die Anonymisierung erlaubt es die Pseudonymisierung, Bezüge zu den betroffenen Individuen in den Datensätzen zu erhalten. Die Idee der Pseudonymisierung besteht darin, diese Zuordnung von Datensatz zu Betroffenem als Geheimnis zu werten, dessen Offenlegung nur unter entsprechenden – wohldefinierten – Bedingungen erfolgen soll. Ein gängiges Verfahren zur Pseudonymisierung besteht folglich etwa darin, jedem Datensatz eine eindeutige, aber zufällig gewählte Nummer – das Pseudonym – zuzuordnen. Die Tabelle mit diesen Nummern und den ihnen zuzuordnenden Betroffenen (bzw. den identifizierenden Daten zu diesen Betroffenen, etwa Name oder E-Mail-Adresse) bildet dann den Pseudonymisierungsschlüssel, der dem Datenverarbeiter der pseudonymisierten Daten im Normalfall nicht zur Kenntnis gegeben werden soll. Die Annahme hier lautet also, dass ein Rückschluss aus den pseudonymisierten Daten auf die zugehörigen Individuen möglich und durchführbar ist, dass die Durchführung dieses Rückschlusses aber durch Geheimhaltung der Zuordnungsvorschrift nur unter kontrollierten Umständen erfolgen kann.

Eine abschließende Aufzählung aller denkbaren Arten von Pseudonymisierungsverfahren ist nicht möglich, da sich – je nach Kontext – unzählige Möglichkeiten zur Pseudonymbildung ergeben. Erwähnenswert ist noch, dass die Zuordnung zwischen Datensatz und Individuum keineswegs nur aus einer einzigen Tabelle hervorgehen muss. Gerade im medizinischen Bereich sind Beispiele bekannt, in denen zwei, drei oder mehr Pseudonymisierungsstufen hintereinander durchgeführt werden, um die Rückverfolgung einzelner Datensätze deutlich zu erschweren.

g. Das Verhältnis von Anonymisierung, Pseudonymisierung und Re-Identifizierung

Die generelle Annahme zur Verarbeitung anonymisierter Datenbestände ist, dass es nicht möglich ist, auch nur eine einzige Information mit direktem Personenbezug aus den anonymisierten Daten zu gewinnen. Folglich reicht die Demonstration einer einzigen Re-Identifizierung, eines einzigen Rückschlusses auf die Identität eines Individuums aus, um den Beweis der Nicht-Anonymität eines Datenbestandes zu erbringen. Interessanterweise gilt dieselbe Art der Beweisführung auch für pseudonymisierte Daten, falls ein Re-

[56] N. Li, T. Li, S. Venkatasubramanian: t-Closeness: Privacy Beyond k-Anonymity and l-Diversity. In: ICDE, Vol. 7, 2007, S. 106-115

Identifizierungsangriff auf derartige Datenbestände ohne Zuhilfenahme der existenten Pseudonymtabellen erfolgreich ist. Ein Beispiel hierfür findet sich etwa in der Veröffentlichung von Suchdaten der Suchmaschine AOL[57]. Hier wurden die – per Identifikationsnummer pseudonymisierten – Suchbegriffe der Nutzer der AOL-Suchfunktion veröffentlicht, unter der Annahme, ein Rückschluss auf die Identität der Suchenden sei durch die Pseudonymisierung nicht ohne Nutzung der Zuordnungstabelle möglich. Die Zuordnungstabelle wurde auch nicht bemüht, vielmehr gelang es einer Gruppe von Wissenschaftlern und Journalisten, durch Zuhilfenahme weiterer öffentlich verfügbarer Datenbestände eine kleine Anzahl von Individuen in der pseudonymisierten Datenmenge zu re-identifizieren. Dies erfolgte allein aufgrund der (englischsprachigen) Suchbegriffe, die diese Nutzer in die AOL-Suchmaschine eingegeben hatten.

Eine essentielle Beobachtung hierbei ist folglich, dass Re-Identifizierungsangriffe sowohl für vermeintlich anonymisierte als auch für pseudonymisierte Datenbestände funktionieren. Darüber hinaus lässt sich ableiten, dass nur die Nicht-Anonymität eines Datenbestandes beweisbar ist, durch einen Nachweis in Form einer entsprechenden Re-Identizierung. Ein Beweis der Anonymität eines Datenbestandes ist nach aktuellem Stand der Forschung nicht bzw. nur in irrelevanten Trivialfällen realisierbar.

E. Datenschutzrechtliche Grundlagen für späteren Einsatz des fertigen Tools

Ausgehend von einem fertig entwickelten „Tool“ zur zuverlässigen Messung von IT-Security-Awareness bei IT-Anwendern in einem Beschäftigungsverhältnis, ist zu prüfen, auf welcher Grundlage ein solches Tool in einem Betrieb bzw. einer Organisation eingesetzt werden dürfte, um das IT-Sicherheitsbewusstsein der Mitarbeiter zu messen.

I. Datenschutzgesetze

1. § 23 LDSG/§ 32 BDSG

§ 23 LDSG S-H und § 32 BDSG regeln in ihren jeweiligen Anwendungsbereichen die Zulässigkeit von Datenverarbeitung in Beschäftigungsverhältnissen. Insofern kann auf die Ausführungen in Dokument 2.1 verwiesen werden.

[57] M. Barbaro, T. Zeller: "A Face Is Exposed for AOL Searcher No. 4417749". The New York Times. 2006.

2. §§ 11 Abs. 1 Nr. 2, 13 Abs. 1 LDSG/§ 4 Abs. 2 Nr. 1 BDSG

Der Abschluss einer Dienst- oder Betriebsvereinbarung ist auch außerhalb von Forschungsvorhaben eine mögliche Datenerhebungsgrundlage. Grundlegendes hierzu findet sich ebenfalls in Dokument 2.1.

3. Einwilligung im Arbeitsverhältnis

Sofern keine gesetzliche Erlaubnisnorm für die konkrete Datenverarbeitung besteht, kann die Datenerhebung und -verarbeitung in der Regel rechtmäßig auf Grundlage der Einwilligung der Betroffenen erfolgen. Von den Beschäftigten könnte mithin eine Einwilligung eingeholt werden, bevor das Tool zum Einsatz kommt.

„Einwilligung“ wird definiert als „jede Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, dass personenbezogene Daten, die sie betreffen, verarbeitet werden.“ (Art. 2 lit. h) Richtlinie 95/46/EG). Die entsprechende landesgesetzliche Umsetzung findet sich in § 12 Abs. 2 LDSG S-H.

„Freiwillig“ setzt dementsprechend voraus, dass die Betroffenen die Möglichkeit haben, abzulehnen. Im Beschäftigungsverhältnis wird regelmäßig bezweifelt, ob Beschäftigte überhaupt „freiwillig“ einwilligen können. Grundsätzlich steht es der „Freiwilligkeit“ entgegen, wenn sich die Beteiligten nicht „auf Augenhöhe“ gegenüberstehen und damit „faktisch ein Machtungleichgewicht besteht“.[58] Ein solches wird regelmäßig bestehen, wenn die Einwilligung für die Ausübung der Arbeitstätigkeit erforderlich ist.

Das Bundesarbeitsgericht[59] indes erachtete im Falle der Einwilligung in die Veröffentlichung von Bildmaterial das auch einen Arbeitnehmer eindeutig identifizierbar abbildete, die Einwilligung auch in Arbeitsverhältnissen für grds. möglich. Es führt hierzu aus, dass sich Arbeitnehmer auch im Rahmen eines Arbeitsverhältnisses können „grundsätzlich ‚frei entscheiden‘“, wie sie ihr Grundrecht auf informationelle Selbstbestimmung ausüben wollen. Dass Arbeitnehmer abhängig Beschäftigte seien und der Arbeitgeber ein Weisungsrecht habe, stünde dem nicht entgegen; Arbeitnehmer begäben sich nicht ihrer Grund- und Persönlichkeitsrechte.[60] Lediglich wenn tatsächlich Benachteiligungen durch die Weigerung der Abgabe einer Einwilligungserklärung eintreten bzw. drohen würden, stelle dies eine Nebenpflichtverletzung des Arbeitgebers dar und löse

[58] Simitis/*Scholz/Sokol*, BDSG, § 4 Rn. 7.
[59] BAG, Urteil vom 11. Dezember 2014, Az. 8 AZR 1010/13.
[60] BAG, a.a.O., Rn. 38.

Schadensersatzansprüche aus.[61] Der insoweit zugrunde liegende Sachverhalt der Veröffentlichung von Mitarbeiterbildnern auf der firmeneigenen Website zu Werbezwecken stellt zugleich ein Beispiel für den grds. zuzulassenden Fall dar, dass eine Verarbeitung nicht für die Ausübung des Arbeitsverhältnisses erforderlich ist und dementsprechend eine tatsächliche Wahlmöglichkeit für den Beschäftigten besteht, bzw. bestehen kann.

II. Weitere Rechtsgrundlagen

1. IT-Sicherheitsgesetz (und die VOen)

Das „IT-Sicherheitsgesetz“ (Gesetz zur Erhöhung der Sicherheit informationstechnischer System; IT-SiG) wurde im Juli 2015 verkündet[62] und trat noch im selben Monat in Kraft.

Das IT-SiG soll ausweislich seiner Zielsetzung[63] IT-Systeme „im Hinblick auf die Schutzgüter der IT-Sicherheit (Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität)“ verbessern. Insbesondere den Betreibern von sog. „Kritische Infrastrukturen“ wird eine besondere „Verantwortung für das Gemeinwohl“ zugeschrieben,[64] weshalb diese durch das IT-SiG zur Einhaltung eines Mindestmaßes von IT-Sicherheit, sowie zur Meldung relevanter Vorfälle an das Bundesamt für Sicherheit in der Informationstechnik (BSI) als „nationale zentrale Stelle für IT-Sicherheit“ verpflichtet werden. Hierzu wurde dem BSI-Gesetz (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik; BSG) durch das IT-SiG mit § 2 Abs. 10 auch eine Definition des Begriffes „Kritische Infrastrukturen“ hinzugefügt. Kritische Infrastrukturen sind demnach „Einrichtungen, Anlagen oder Teile davon, die den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und“ zudem „von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.“ Während ohnehin die allgemeine Abhängigkeit der Gesellschaft, Wirtschaft, Verwaltung und Gesundheitsversorgung von IT-Systemen zunimmt, ist diese Abhängigkeit im Falle von „Kritischen Infrastrukturen“ sogar existenziell.[65]

---

[61] BAG, a.a.O., Rn. 38 a.E.
[62] BGBl. I 2015, 1324; online verfügbar: http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*%255B@attr_id=%27bgbl115s1324.pdf%27%255D#__bgbl__%2F%2F*[%40attr_id%3D%27bgbl115s1324.pdf%27]__1453708895167
[63] BT-Drucks. 18/4096, S. 1.
[64] BT-Drucks. 18/4096, S. 2; BT-Drucks. 18/5121, S. 2.
[65] *Roßnagel*, DVBl. 2015, 1206 (1206).

Wann genau in den einzelnen Sektoren Betreiber von Anlagen oder Teilen davon „kritische Dienstleistungen“ ausübt, wird im Verordnungswege (Rechtsverordnungen entsprechend der Ermächtigung § 10 Abs. 1 IT-SiG) festgelegt. Während zum Zeitpunkt der Erstellung dieses Dokuments bereits ein Verordnungsentwurf für die Sektoren Energie, Wasser, Ernährung, Informationstechnik und Telekommunikation vorliegt,[66] gibt es zu den Sektoren Gesundheit und Finanz- und Versicherungswesen noch keine Entwürfe. Solche sollen bis Ende 2016 vorgelegt werden.[67]

Aus dem vorliegenden Entwurfstext geht hervor, dass die Beurteilung, ob es sich bei Anlagen oder Teilen davon um „Kritische Infrastrukturen“ handelt, von branchenspezifischen Schwellenwerten abhängig gemacht wird. (Vgl. etwa zum Sektor Informationstechnik und Kommunikation § 5 Abs. 4 Nr. 2 BSI-Kritisverordnung; BSIKritisV). Diese einzelnen Schwellenwerte werden berechnet unter Zugrundelegung eines „Regelschwellenwertes“ von 500.000 Personen. Anlagen, die nicht mindestens 500.000 Personen versorgen, scheiden im Umkehrschluss bereits aus diesem Grunde als „Kritische Infrastruktur“ aus.

Soweit das UKSH als Telekommunikationsanbieter seinen Beschäftigten gegenüber einzuordnen ist (vgl. Dokument 2.1 –Arbeitsrechtliche Betrachtung) scheidet es mithin im Hinblick auf Telekommunikation bereits aus dem Grund als Betreiber einer kritischen Infrastruktur aus; 500.000 Beschäftigte werden nicht erreicht.

Das UKSH als Universitätsklinikum gehört dem Sektor Gesundheit an und hat als Einrichtung der Maximalversorgung einen sehr weiteren Einzugskreis in Schleswig-Holstein. Einzelne Abteilungen oder Einrichtungen des UKSH werden vorraussichtlich als „Kritische Infrastrukturen“ einzuordnen sein. Fehler in der IT, die zur Folge hätten, dass eine Versorgung der Patienten an den betroffenen Behandlungsplätzen nicht optimal gewährleistet ist, würden bedeuten, dass die Behandlungsplätze nicht zur Verfügung stehen. Dies würde wiederum zu Versorgungsengpässen führen. Allerdings ist zum Zeitpunkt der Erstellung des Dokuments die Verordnung über die Voraussetzungen zur Einordnung als kritische Infrastruktur für den Bereich Gesundheit noch nicht veröffentlicht.

Aus dem IT-SIG ergeben sich für die Erhebung und Verarbeitung von personenbezogenen Daten im Rahmen von IT-Security-Awareness-Tests der Beschäftigten im UKSH im Ergebnis keine (weiteren) Rechtsgrundlagen oder Besonderheiten.

[66] http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/kritis-vo.pdf?__blob=publicationFile
[67] http://www.heise.de/newsticker/meldung/IT-Sicherheitsgesetz-Wer-was-wann-zu-melden-hat-3096885.html

2. TKG

Sofern man das UKSH gegenüber seinen Beschäftigten als Telekommunikationsdiensteanbieter betrachtet (vgl. Dokument 2.1 – Arbeitsrechtliche Betrachtung), sind auch die einschlägigen Normen des TKG als mögliche Rechtsgrundlagen für den Einsatz eines zukünftigen ITS.APT-Tools in Betracht zu ziehen. Für die Testdurchführung im Rahmen des Projektes hingegen dürfte sich (allein schon mangels bereits erwiesener Wirksamkeit) noch keine Grundlage im TKG finden. § 100 Abs. 1 TKG gestattet, „soweit erforderlich“, die Erhebung und Verwendung von Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer, um Störungen oder Fehler an Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen.

Die Norm fokussiert auf den Erhalt der Funktionsfähigkeit der Telekommunikationsanlage selbst. Ein „Fehler“ liegt vor, wenn die Anlage in dem Sinne nicht mehr ordnungsgemäß funktioniert, dass es zu Fehlern bei der Übertragung von Nachrichten kommt.[68]

Eine „Störung“ liegt nach der weiten Auslegung des BGH[69] z.B. bereits vor, wenn „Internetdienstleister bestimmte IP-Adressbereiche eines anderen Internetanbieters sperren, weil von ihnen Schadprogramme oder massenweise sog. Spam-Mails versandt werden oder „Denial-of-Service-Attacken“ ausgehen“.[70] Dieses Sperren sei eine Veränderung der Telekommunikationsanlagen, die sodann nicht mehr nutzbar seien. Es wird mittelbar ein berechtigtes Interesse des Anlagenbetreibers, Spam-Mails von seiner Anlage fernzuhalten anerkannt.

Aber in jedem Falle muss das Speichern personenbezogener Daten in diesem Zusammenhang dem „Erkennen, Eingrenzen oder Beseitigen“ der Störung oder des Fehlers dienen. Auch wenn nur die Varianten „Eingrenzen“ und „Beseitigen“ klar bereits eine bestehende Störung bzw. einen Fehler voraussetzen,[71] ist doch auch die Variante „Erkennen“ im Zusammenhang mit realen Störungen oder Fehlern zu lesen. Für den hier vorliegenden Fall kann die Norm mithin keine Datenerhebungsgrundlage sein: Die Messung von Nutzerreaktionen auf falsche Spam-Mails – wenn auch mit dem Ziel sie anschließend zu schulen – ist nicht unmittelbar „erforderlich“ für das Erkennen von Störungen und Fehlern.

Zwar soll es genügen, dass die Datenerhebung und –verwendung geeignet, erforderlich und im engeren Sinn verhältnismäßig ist, um „abstrakten Gefahren für die

[68] BeckTKG/, TKG § 100 Rn. 8.
[69] Vgl. BGH Urteil vom 13.01.2011, Az. III ZR 146/11.
[70] BGH Urteil vom 13.01.2011, Az. III ZR 146/11, Rn. 35.
[71] BeckTKG/*Braun*, § 100 Rn. 9.

Funktionstüchtigkeit des Telekommunikationsbetriebs entgegenzuwirken“,[72] d.h. ein konkreter Vorfall bzw. Verdacht wird nicht vorausgesetzt. Aber dennoch wird auf ein Sammeln von „Anhaltspunkten“ zum „Erkennen“ von Fehlern und Störungen abgestellt.[73] Wie ein Beschäftigter auf eine manipulierte Spam-Mail reagiert, steht hiermit nicht in ausreichend engem Zusammenhang. In diesem ersten Schritt – der Datenerfassung – geht es lediglich um die Feststellung der Nutzerreaktion. Dies ist ein dem eigentlichen Normzweck weit vorgelagerter Schritt. Dass eine Nutzerreaktion zu einer Störung bzw. einem Fehler der Telekommunikationsanlage führen könnte, wenn es sich um eine echte Spam-Mail handeln würde (etwa durch fahrlässiges Herunterladen eines Schadprogrammes), kann nicht das gezielte, bis zu sieben Tagen dauernde,[74] „Tracken“ von Beschäftigten gestatten.

3. TMG

Um zu einer Anwendbarkeit des Telemediengesetzes (TMG) für den Bereich Mitarbeiter-E-Mail zu gelangen, müsste es sich beim UKSH zunächst um eine Stelle handeln, die „Telemedien“ „zur Nutzung bereithält“ bzw. „den Zugang zur Nutzung vermittelt“ (Telemedien-)Diensteanbieter im Sinne des Gesetzes würde (§ 2 Nr. 1 TMG).

Der Anwendungsbereich des TMG ist in § 1 Abs. 1 TMG negativ definiert. Telemedien sind demnach „alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 des Telekommunikationsgesetzes [sind], die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, [sowie] telekommunikationsgestützte Dienste nach § 3 Nr. 25 des Telekommunikationsgesetzes oder Rundfunk nach § 2 des Rundfunkstaatsvertrages“ (§ 1 Abs. 1 S. 1 TMG).

Für die Bestimmung eines Dienstes als „Telemedien“ ist mithin nicht die Form der Übertragung – wie wird Zugang gewährt, wie werden die für die Diensterbringung relevanten Daten übermittelt – entscheidend, sondern die für den Dienst erforderlichen Inhalte. Diese müssen elektronisch zur Verfügung gestellt werden.[75] Unerheblich ist, ob der Anbieter diese als eigene Telemedien (Content-Provider) oder bloß Serverkapazitäten für fremde Telemedien zur Verfügung stellt und so diese zur Nutzung bereithält (Host-Provider bzw. Service-Provider).[76] Typische Beispiele für Telemedien sind etwa Suchmaschinen, Informationsdienste, Webmail-Dienste etc.[77] Hinsichtlich des „Diensteanbieters“

[72] BGH Urteil vom 13.01.2011, Az. III ZR 146/11, Rn. 36.
[73] BGH Urteil vom 13.01.2011, Az. III ZR 146/11, Rn. 39.
[74] Vgl. BGH zur nach § 100 TKG gestatteten Dauer.
[75] Spindler/Schuster/*Ricke*, TMG, § 1 Rn. 4.
[76] BeckOK InfoMedienR/*Martini*, TMG, § 2 Rn. 7.
[77] *Brink*, ZD 2015, 295 (296).

unterscheidet § 1 Abs. 1 S. 2 TMG nicht zwischen privaten und öffentlichen Angeboten, bzw. auch nicht zwischen entgeltlichen und unentgeltlichen. Die sich aus dem TMG ergebenden Pflichten sind mithin von privaten, wie öffentlichen Anbietern zu beachten.[78] Das UKSH könnte daher als Anbieter solcher Dienste betrachtet werden, da es z.B. für einen Teil der Mitarbeiter Webmail-Konten führt. Aus der Tatsache, dass die IT-Infrastruktur durch die IT-Service-GmbH – einen „Dritten" – angeboten wird, ergibt sich keine abweichende Wertung. Im Hinblick auf die Rechte der Beschäftigten ist die GmbH ist lediglich Auftragnehmerin des Diensteanbieters UKSH.

Allerdings ist die Anwendbarkeit des TMG – wie auch die des TKG[79] – im Arbeitgeber-Arbeitnehmer-Verhältnis umstritten, soweit die (auch) private Nutzung von Internet und dienstlicher E-Mail-Adresse den Arbeitnehmern gestattet wird. Im Kern geht es um die Frage, ob der Arbeitgeber an das Fernmeldegeheimnis gebunden ist, bzw. dessen einfachgesetzliche Umsetzung, hier § 88 Abs. 2 S. 1 TKG i.V.m. § 7 Abs. 2 S. 3 TMG.[80]

Gegen die Anwendung wird ausgeführt, dass die Mitarbeiter dann auch als „Nutzer" im Sinne des TMG anzusehen sein müssten. Nutzer ist „jede natürliche oder juristische Person, die Telemedien nutzt, insbesondere um Informationen zu erlangen oder zugänglich zu machen" (§ 2 Nr. 3 TMG), d.h. wer sich Inhalte ansieht, abruft oder herunterlädt, d.h. die Angebote in irgendeiner Weise nachfragt.[81] Der Arbeitnehmer, der im Rahmen eines Dienst- oder Arbeitsverhältnisses auf Telemedien zugreift, ist nach einer in der Literatur vorherrschenden Auffassung kein „Nutzer" im Sinne des Gesetzes, da es bei nur dienstlich gestatteter Nutzung an der Eigenverantwortlichkeit der Nutzung mangelt.[82] Im Falle der Nichtanwendbarkeit des TMG sind die allgemeinen Datenschutzgesetze anzuwenden.

Im UKSH ist die private Nutzung untersagt, sodass die Fragevorliegend für das Ergebnis nicht relevant ist und nicht abschließend zu beantworten ist. . Speziell zu den datenschutzrechtlichen Bestimmungen des TMG sei Folgendes ergänzend erwähnt: Der hier zu beurteilenden Sachverhalt weist die Besonderheit auf, dass es um die Anwendbarkeit des TMG – bzw. seiner datenschutzrechtlichen Bestimmungen – im Verhältnis Arbeitgeber-Arbeitnehmer geht, d.h. das UKSH in seiner Eigenschaft als Arbeitgeber gegenüber den Mitarbeitern. Anders als das TKG enthält das TMG mit § 11 Abs. 1 Nr. 1 eine Norm, die explizit die Bereitstellung von Telemediendiensten im Dienst- und Arbeitsverhältnis regelt.

[78] Spindler/Schuster/*Ricke*, TMG, § 1 Rn. 14.
[79] Zur Anwendbarkeit des TKG im Arbeitgeber-Arbeitnehmer-Verhältnis vgl. Dokument 2.1, S. 12 ff.
[80] *Brink*, ZD 2015, 295 (296).
[81] Spindler/Schuster/*Ricke*, TMG, § 2 Rn. 8.
[82] Spindler/Schuster/*Ricke*, TMG, § 2 Rn. 8.

Hiernach gelten die Vorschriften des Abschnittes 4 (Datenschutz) nicht, soweit die Bereitstellung „im Dienst- und Arbeitsverhältnis zu ausschließlich beruflichen oder dienstlichen Zwecken“ erfolgt. Die §§ 14, 15 TMG, Die Voraussetzung der „Ausschließlichkeit“ wird als erfüllt angesehen, wenn der Arbeitgeber dem Arbeitnehmer die private Nutzung des Internets bzw. der dienstlichen E-Mail-Adresse untersagt.[83]

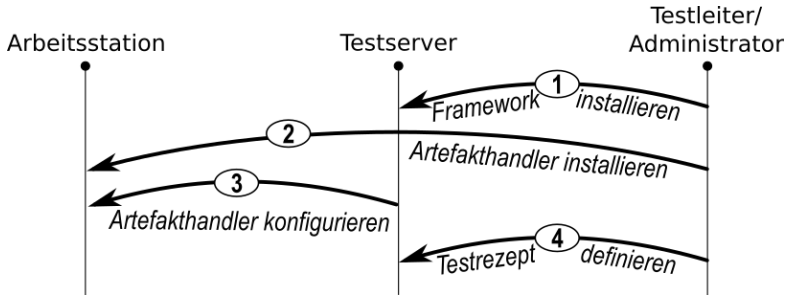
F. Technische Umsetzung

Das zuvor Gesagte muss auch technisch umgesetzt werden. Um dies datenschutzfreundlich zu gestalten, sollten die im Folgenden beschriebenen Schritte eingehalten werden. In diesem Abschnitt wird die Experimentdurchführung im Einzelnen beschrieben.

Der technische Ablauf der ersten und dritten Stufe soll in weitgehend identischer Art und Weise erfolgen, und untergliedert sich jeweils in vier verschiedene Phasen. Hinsichtlich der datenschutzrechtlichen Analyse der hierbei auftretenden Sachverhalte sind dabei die Einzelheiten eben dieser vier Phasen relevant, die im Folgenden genauer aufgeführt werden.

I. Installationsphase

Um die Durchführung des Experimentes bzw. der Messungen an den Arbeitsplätzen der Probanden in geeigneter Weise vornehmen zu können, müssen deren Computer vor Beginn der ersten Testphase geeignet vorbereitet werden. Konkret erforderlich sind folgende Arbeitsschritte:



1. Das ITS.APT-Testframework muss auf dem für die Testdurchführung vorgesehenen Testserver installiert werden. Dies erledigt üblicherweise ein Administrator auf Anweisung des Testleiters. Der Testserver dient dabei sowohl als serverseitige Komponente bei der Einspielung sicherheitsrelevanter Anzeigen bei den Probanden (Einbringung sog. Artefakte), etwa beim Versand von SPAM-Mails, als auch als Sammel- und Protokollierungsstelle für die aufgezeichneten Probandenreaktionen.

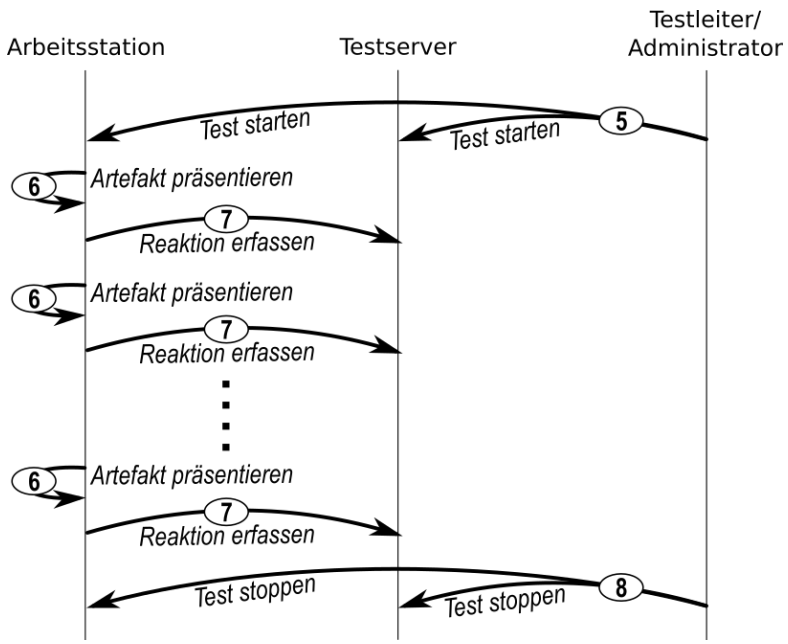
[83] BeckOK InfoMedienR/*Martini*, TMG § 2 Rn. 10.

2. Auf den Arbeitsplatz-Computern der Probanden wird in diesem Arbeitsschritt die ITS.APT-Software installiert, die zur Steuerung der Anzeige von Artefakten sowie zur Protokollierung und Übertragung der jeweiligen Probandenreaktionen an den Testserver erforderlich ist. Auch dieser Schritt wird von einem Administrator auf Weisung des Testleiters durchgeführt.
3. In diesem optionalen Arbeitsschritt werden die verschiedenen Arbeitsplatz-Computer der Probanden beim Testserver registriert bzw. von diesem vorkonfiguriert, um im späteren Verlauf die notwendige Kommunikation zwischen Testserver und Arbeitsplatz-Computern optimal steuern zu können. Wie in den ersten beiden Arbeitsschritten erfolgt dies durch einen Administrator auf Weisung des Testleiters, sowie teilweise vollautomatisch durch die interne Kommunikation der verschiedenen Komponenten des ITS.APT-Frameworks.
4. Im letzten Arbeitsschritt der Installationsphase definiert der Testleiter auf dem Testserver die durchzuführenden Testläufe (sog. *Testrezept*) hinsichtlich
    a. Vorgesehener Dauer des Testlaufes
    b. Vorgesehener Liste von Probanden für den Testlauf
    c. Vorgesehener Liste von Arbeitsplatz-Computern für den Testlauf
    d. Vorgesehener Typen von Artefakten

Die Arbeitsschritte 1. und 2. sind dabei nur vor der ersten Testdurchführung bzw. in der ersten Experimentstufe zu vollziehen. Für den zweiten Testdurchlauf, in Stufe 3, sind nur Arbeitsschritt 4. und ggfs. Arbeitsschritt 3. erneut durchzuführen.

II. Durchführungsphase

In der Durchführungsphase werden die vorab installierten und konfigurierten Artefakte aktiv ausgeführt. Hierbei werden die Probanden unter definierten Umständen mit einem (visuellen, akustischen, o.Ä.) Artefakt konfrontiert, und ihre jeweilige Reaktion darauf wird protokolliert. Im Einzelnen ergeben sich folgende Arbeitsschritte:



5. Das Signal zum Start eines Testlaufes geht auf den Testleiter zurück. Die genaue Abfolge kann hier im Einzelnen abweichen, etwa, wenn das Startsignal an die Arbeitsstationen nicht direkt vom Testleiter sondern vom Testserver weitergeleitet wird. Auch kann hier eine vorab konfigurierte zeitliche Steuerung den tatsächlichen Startzeitpunkt eines Durchlaufes definieren, dieser ist dann aber vorab vom Testleiter als zuständige (und ggfs. verantwortliche) Position konfiguriert worden. Ab diesem Zeitpunkt läuft das Experiment.
6. Während des Experimentes werden – ausgelöst durch zeitliche, arbeitsbedingte oder zufallsbasierte Trigger – die einzelnen im Testrezept definierten und konfigurierten Artefakte ausgeführt. Hierdurch wird jedes Mal (mindestens) ein Proband mit einer dem jeweiligen Artefakt zuzuordnenden Anormalität konfrontiert.
7. Nach Präsentation der jeweiligen Artefakte wird die Reaktion des/der Probanden auf diese Artefakte bestmöglich erhoben und auf dem Testserver protokolliert. Hierzu ist eine Datenübertragung zwischen Arbeitsstation und Testserver erforderlich, die artefaktrelevante Daten enthält, unter anderem:
    a. Datum und Uhrzeit,
    b. Identität der Arbeitsstation,
    c. Informationen über den Probanden (z.B. Benutzername),
    d. Typ des Artefakts,
    e. auf der Arbeitsstation lokal erfasste Reaktion des Probanden (z.B. Fenster schließen),
    f. Reaktionszeit zwischen Artefaktpräsentation und Reaktion

Je nach Konfiguration der technischen Infrastruktur ist in diesem Schritt unter Umständen auch der Einbezug weiterer relevanter technischer Systeme erforderlich. Beispielsweise kann es erforderlich werden, folgende Zusatzdaten aus Drittsystemen zu erheben und dem Testserver zur Protokollierung zuzuleiten:

a. Identität des Probanden (z.B. aus einem zentralen Benutzerverzeichnis)
b. externe bzw. nicht direkt erfassbare Reaktion des Probanden (z.B. Anruf bei einer Support-Hotline)
c. Identität der Arbeitsstation (z.B. in stark virtualisierten Umgebungen)

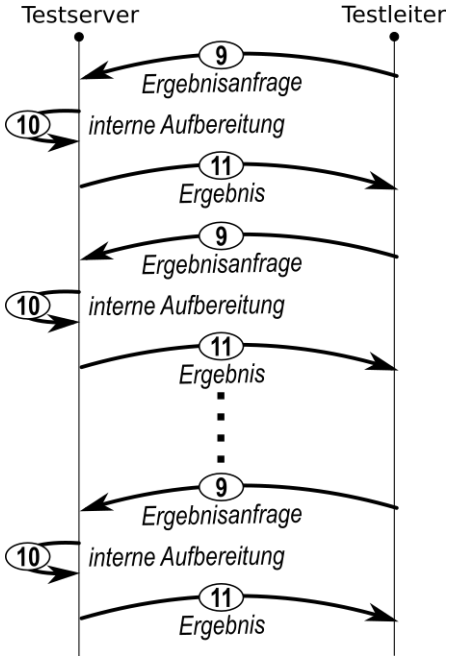
Die Arbeitsschritte 6. und 7. werden für jedes Artefakt bzw. für jede Präsentation eines Artefaktes während der Testdauer wiederholt.

8. Der Testdurchlauf wird in diesem Arbeitsschritt gestoppt. Ein derartiger Stopp kann auf zwei verschiedenen Wegen erfolgen. Entweder erreicht der Testdurchlauf den vorab vom Testleiter definierten Abschlusszeitpunkt, oder der Testleiter unterbricht die Testdurchführung aktiv durch Auswahl der entsprechenden Aktion aus der Bedienungsoberfläche des Testservers. In beiden Fällen werden die aktuell laufenden Instanzen der Arbeitsschritte 6. und 7. noch vollendet, es werden aber keine weiteren Artefaktpräsentationen mehr gestartet. Das Signal zur Beendigung des Tests kann dabei entweder durch den Testserver an die Arbeitsstationen verteilt werden oder es kann durch den Testleiter bzw. durch Administratoren manuell lokal auf den Arbeitsstationen erfolgen.

Mit Abschluss des 8. Arbeitsschrittes endet die Durchführungsphase.

III. UKSH-Interne Evaluation

Die interne Evaluation bzw. Aufbereitung der gesammelten Reaktionsdaten der Probanden geschieht teilweise während, spätestens aber nach Abschluss der Durchführungsphase. Ziel dieser Phase ist es, gezielt Informationen aus der Aggregation der gesammelten Daten zu gewinnen, etwa in Form statistischer Werte. Hierfür werden wiederholt die folgenden Arbeitsschritte durchgeführt:



9. Ausgelöst durch eine Aktion des Testleiters wird eine Datenanfrage nach bestimmten Datensätzen (oder Operationen auf diesen Datensätzen) an den Testserver übermittelt, auf welchem die gesammelten Reaktionsdaten der Probanden vorliegen. Gegebenenfalls werden hierbei entsprechende Eingabeparameter zur Ermittlung des jeweiligen Ergebnisses übertragen, beispielsweise:

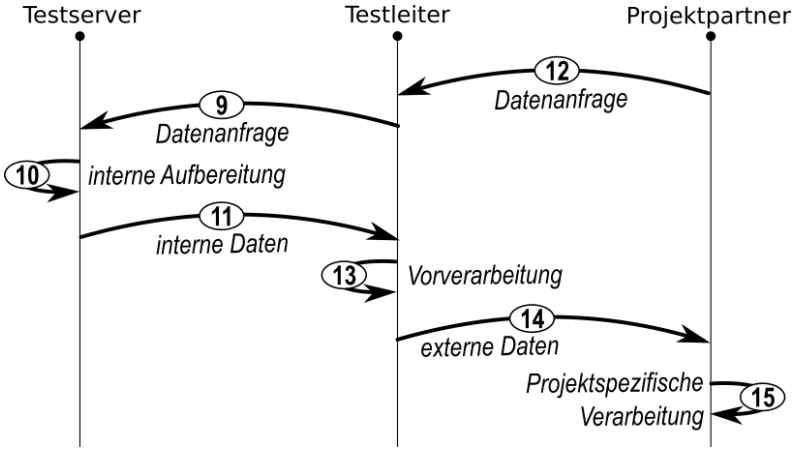
    a. zu betrachtender Zeitraum
    b. zu betrachtende Liste von Probanden
    c. zu betrachtende Liste von Arbeitsstationen
    d. zu betrachtende Liste von Artefakttypen
    e. zu betrachtende Liste von Reaktionstypen

10. Im Rahmen einer programminternen Auswertung werden die angeforderten Daten nach Maßgabe der Parameter aus dem vorigen Arbeitsschritt abgerufen, aufbereitet und für die Rückübertragung vorbereitet, bzw. gemäß der Art der angeforderten Operation vorverarbeitet. Dieser Arbeitsschritt greift dabei auf die vollständige Datenbank mit Probandenreaktionen zu, die im Klartext als Rohdaten vorliegen.
11. Nach Ausführung entsprechender Aggregations- und Aufbereitungsoperationen wird das Ergebnis der Anfrage an den anfragenden Testleiter zurückgegeben bzw. in geeigneter Form (z.B. im Browser) dargestellt.

Die Arbeitsschritte 9. bis 11. werden je nach Bedarf wiederholt durchgeführt. Die so gewonnenen Erkenntnisse können auf Seiten des Testleiters für weitere Verarbeitungsschritte (z.B. für visuelle Aufbereitung) verwendet werden.

IV. Projektseitige Evaluation

Ausgehend von der Zielstellung des ITS.APT-Projektes und den entsprechenden Anfragen der Projektpartner werden in dieser Phase die Datenbestände aus der Durchführungsphase für die weitere Verwendung im Projektkontext bereitgestellt. Hierbei ist relevant, dass durch das UKSH stets eine Vorabkontrolle der zu übermittelnden Daten erfolgt, da hier ggfs. eine organisatorische Domäne (Einflussbereich des UKSH) verlassen wird. Im Einzelnen erfolgen hierbei folgende Arbeitsschritte:



12. Ausgehend von den für die Erzielung des Projektergebnisses erforderlichen Informationen werden durch die Projektpartner Anfragen zu bestimmten Daten über die Probandenreaktionen definiert und an den Projektpartner UKSH in Gestalt des Testleiters übermittelt. Der Testleiter nutzt dann die in Arbeitsschritt 9. bis 11. bestehenden Möglichkeiten zur UKSH-internen Evaluation, um die zur Beantwortung der Anfragen erforderlichen Datenbestände und Informationen zusammenzutragen. Hierfür ist ggfs. eine mehrfache Durchführung der besagten Arbeitsschritte erforderlich.
13. Hat der Testleiter sämtliche erforderlichen Daten zur Beantwortung der spezifischen Projektanfrage zusammengetragen, ist gegebenenfalls eine UKSH-interne Vorverarbeitung dieser Daten erforderlich. Dies kann etwa notwendig werden, um
    a. Personenbezug aus den Daten zu entfernen,
    b. Daten anderweitig zu anonymisieren oder zu pseudonymisieren,
    c. Daten mittels weiterer Informationsquellen zu verifizieren,
    d. Statistische Operationen auf gesammelten Eingabedaten durchzuführen,

e. relevante Begleitinformationen zu den Daten und ihrem Erhebungskontext zu identifizieren und dem Anfrageergebnis entsprechend beizufügen

14. Nach entsprechender Vorverarbeitung werden die Ergebnisse zur Anfrage an die entsprechenden Projektpartner übermittelt. Hierbei verlassen sie die Einflussdomäne des UKSH.
15. Nach Überstellung der Anfrageergebnisse an den anfragenden Projektpartner erfolgt dort die weitere Auswertung nach Maßgabe des Projektplans.

G. Gewährleistung der Betroffenenrechte

Die datenschutzrechtlichen Betroffenenrechte sind bei jeder automatisierten Verarbeitung personenbezogener Daten zu gewährleisten. Im Einzelnen handelt es sich – in der Terminologie des LDSG S-H – um Aufklärung und Benachrichtigung, Auskunft, Berichtigung, Einwand, sowie Löschung und Sperrung. Auch das Recht auf Schadenersatz ist grds. ein Betroffenenrecht. Letzteres wird ausführlich in dem Dokument 2.2 – Haftungsrechtliche Betrachtung behandelt. Die in §§ 33 ff. BDSG, bzw. §§ 26 ff. LDSG S-H geregelten Betroffenenrechte dienen hinsichtlich Information, Benachrichtigung, Berichtigung und Löschung der Umsetzung der Art. 10-12 der Richtlinie 95/46/EG, sowie hinsichtlich des Einwandes der Umsetzung des Art. 14 Richtlinie 95/46/EG.

I. Anspruchsgegner

Die Betroffenenrechte bestehen gegenüber der datenverarbeitenden Stelle. Im Projektkontext ist dies zunächst das UKSH (vgl. bereits oben). Aber durch Übermittlung der durch das UKSH erhobenen Daten an andere Projektpartner, werden diese Projektpartner ebenso zu datenverarbeitenden Stellen und somit zu Anspruchsgegnern für die Betroffenen. Die Datenerhebung kann auch im willentlichen oder selbst veranlassten Empfang bereits anderweitig erhobener Daten bestehen.[84] Sie umfasst nicht nur die originäre Erhebung (durch jemand anderen).[85] Für keinen Projektpartner außer UKSH und ULD gilt das LDSG S-H, sondern – je nach ihrer Organisationsform – das BDSG oder das LDSG ihres jeweiligen Bundeslandes (vgl. C.). Die Betroffenenrechte sind jedoch im Grundsatz in allen deutschen Datenschutzgesetzen vergleichbar ausgestaltet.[86]

[84] Simits/*Sokol/Scholz*, BDSG, § 13 Rn. 11.
[85] Simits/*Sokol/Scholz*, BDSG, § 13 Rn. 11.
[86] BeckOK DatenSR/*Schmidt-Wudy*, BDSG, § 6 Rn. 7.

Vorliegend ist insbesondere zu beachten, dass die anderen Projektpartner lediglich pseudonymisierte Daten erhalten werden. Wenn sich die Betroffenen direkt an die Projektpartner als datenverarbeitende Stellen wenden, können diese ohnehin nur unter der Voraussetzung bspw. Auskunft über die über sie gespeicherten Daten erteilen, dass die Betroffenen ihr Pseudonym kennen und dem Projektpartner bei ihrem Auskunftsverlangen nennen. Bei pseudonymisierten Daten ist die verantwortliche Stelle nur zur Auskunft verpflichtet, wenn sie oder eine ihr gegenüber weisungsabhängige Stelle in der Lage ist, das Pseudonym aufzulösen.[87] Da der Informations-/Auskunftsanspruch gegenüber dem UKSH selbstverständlich auch das Pseudonym umfasst, ist es rechtlich geboten und organisatorisch möglich, dass den Betroffenen ihre jeweiligen Pseudonyme durch das UKSH mitgeteilt und sie so in die Lage versetzt werden, von den weiteren Projektpartnern Auskunft zu verlangen. Allerdings sollten die Betroffenen, wenn sie unter Angabe ihres Pseudonyms und ihres Klarnamen oder anderer sie identifizierender Angaben ein solches Auskunftsverlangen stellen, vor Auskunftserteilung darauf hingewiesen werden, dass ihre Pseudonymität gegenüber dem Projektpartner dann nicht mehr gewährleistet ist. Möchte der Betroffene dennoch Auskunft erhalten, ist sie zu erteilen.

II. Aufklärung und Benachrichtigung, § 26 LDSG S-H

Bei Erhebung personenbezogener Daten mit Kenntnis der Betroffenen sind diese „in geeigneter Weise“ nach § 26 Abs. 1 LDSG S-H über folgende Umstände der Datenverarbeitung aufzuklären: die datenverarbeitende Stelle, den Zweck der Datenverarbeitung, die Rechtsvorschrift, die die Datenverarbeitung gestattet (bzw. über die Freiwilligkeit der Datenangabe, sofern keine Rechtsvorschrift existiert), die Folgen einer Nichtbeantwortung, wenn die Angaben für die Gewährung einer Leistung erforderlich sind, die Rechte der Betroffenen, die sich aus dem LDSG S-H ergeben, den Empfängerkreis bei beabsichtigten Übermittlungen und schließlich die Auftragnehmenden, sofern eine Auftragsdatenverarbeitung beabsichtigt wird.

Sofern die Datenerhebung ohne Kenntnis der Betroffenen erfolgt, sind sie gem. § 26 Abs. 3 LDSG S-H „in angemessener Weise über die verarbeiteten Daten“ zu unterrichten. Inhaltlich sind ihnen dabei die datenverarbeitende Stelle, die zugrundeliegende Rechtsvorschrift (bzw. die Freiwilligkeit der Datenverarbeitung), die Folgen der Nichtbeantwortung sofern es um Leistungsgewährung geht und die Betroffenenrechte nach

[87] Däubler/Klebe/Wedde/Weichert/*Däubler*, BDSG, § 34 Rn. 8.

dem LDSG mitzuteilen. Diese Pflicht besteht nicht, wenn die Benachrichtigung unmöglich ist oder einen unverhältnismäßigen Aufwand erfordert.

„Kenntnis“ setzt in diesem Zusammenhang eine Information der Betroffenen über alle Umstände der Datenverarbeitung voraus, die in einer Benachrichtigung enthalten wären.[88]

Im Kontext der Projektdurchführung ist fraglich, inwiefern dies gewährleistet werden kann, ohne den Forschungszweck zu gefährden. Dies gilt insbesondere für eine genaue Angabe des Zwecks der Datenverarbeitung. Es sind grundsätzlich alle Zwecke anzugeben, die die verantwortliche Stelle im Zeitpunkt der Erhebung verfolgt und derart, dass der Betroffene den Hinweis versteht.[89] Bei wissenschaftlicher Forschung allgemein wird mit der Datenverarbeitung i.d.R. nicht auf eine konkrete Maßnahme gegenüber einer Person abgezielt, sondern auf die Erlangung wissenschaftlicher Erkenntnisse, ohne dass darüber hinaus ein Interesse an der Person bestünde. Dennoch bleiben die Betroffenenrechte unverändert bestehen.[90] Anders als nach BDSG (vgl. § 33 Abs. 2 Nr. 5 BDSG) besteht nach LDSG S-H keine Ausnahme von der Benachrichtigungspflicht bei Speicherung und Übermittlung für Zwecke der wissenschaftlichen Forschung. Nach § 26 Abs. 3 S. 2 LDSG S-H entfällt die Pflicht allgemein wenn die Benachrichtigung der Betroffenen unmöglich ist oder einen unverhältnismäßigen Aufwand erfordert. Das ist im vorliegenden Fall nicht gegeben, da wenigstens über die dienstliche E-Mail-Adresse alle Betroffenen erreicht werden können und es sich auch nicht um eine so große Masse an Betroffenen handelt, als dass die Benachrichtigung unverhältnismäßig aufwändig wäre.[91]

Vorliegend besteht die Gefahr, dass das exakte Verständnis der Betroffenen des Erhebungszwecks (und damit des Projektzwecks) aber potenziell die Reaktionen auf die Tests verfälschen.[92] Die Zweckangabe sollte daher möglichst allgemein erfolgen. Allerdings muss die Dienstvereinbarung zugleich den an eine „andere Rechtsnorm“ i.S.d. §§ 11 Abs. 1 Nr. 2, 13 Abs. 1 LDSG S-H zu stellenden Anforderungen gerecht werden, um eine wirksame Erhebungsgrundlage darzustellen. Im Ergebnis bedeutet dies, dass alle Angaben, die im Rahmen der Aufklärungspflicht zu machen sind (und weitere), in der Dienstvereinbarung enthalten sein werden.[93]

[88] Vgl. zum BDSG: Gola/Schomerus/Körffer/*Gola/Klug*, BDSG, § 33 Rn. 6; siehe auch bereits Dokument 2.1 zur Datenerhebung.
[89] Vgl. zum BDSG: Gola/Schomerus/Körffer/*Gola/Klug/Körffer*, BDSG, § 4 Rn. 31.
[90] *Mayen*, NVwZ 1997, 446 (446).
[91] Vgl. zum BDSG: BeckOK DatenSR/*Forgó*, BDSG, § 33 Rn. 60.
[92] Vgl. Dokument 2.1.
[93] Vgl. zu den Anforderungen an eine Dienstvereinbarung Dokument 2.1, S. 27 ff.

Fraglich ist, ob die an eine „Benachrichtigung“ zu stellenden Voraussetzungen erfüllt werden. Grds. setzt eine Benachrichtigung voraus, dass die Betroffenen von ihrem Inhalt Kenntnis nehmen und ihn verstehen können.[94] Schriftlichkeit ist gesetzlich nicht vorgesehen. Zu Beweiszwecken ist empfiehlt sich regelmäßig jedoch die Text- oder Schriftform.[95]

Vorliegend werden die Betroffenen im Rahmen der arbeitsrechtlichen Publizitätspflicht Kenntnis vom Inhalt der Dienstvereinbarung, welche die Datenerhebung regeln wird, nehmen können und somit die Möglichkeit haben, sich über alle gesetzlich maßgeblichen Aspekte zu informieren. Im UKSH werden Dienstvereinbarungen im Intranet bereitgestellt. Grundsätzlich könnten damit alle Beschäftigten Kenntnis von den genauen Umständen der Datenverarbeitung nehmen. Allerdings erfüllt eine solche „öffentliche Mitteilung“ wie etwa ein Aushang nicht die formalen Anforderungen einer Benachrichtigung.[96] Die Beschäftigten könnten mithin mit einem an sie adressierten, verschlossenen Brief benachrichtigt werden oder aber – sofern elektronische Form für ausreichend erachtet wird – mittels einer verschlüsselten E-Mail an ihre dienstlichen E-Mail-Adressen,[97] die jeweils die Dienstvereinbarung oder aber die relevanten Auszüge enthalten müssen.

Die Projektpartner, welche die pseudonymisierten Daten durch das UKSH übermittelt bekommen, müssen die Betroffenen nicht (erneut) benachrichtigen: Gem. § 26 Abs. 1 S. 2 LDSG S-H ist eine Benachrichtigung nicht erforderlich, wenn den Betroffenen die Informationen bereits vorliegen. Das ist mit den bereits vorliegenden Darstellungen in der Dienstvereinbarung gegeben.

III. Auskunft, § 27 LDSG S-H

Es besteht ein Recht der Betroffenen auf Auskunft gegenüber der datenverarbeitenden Stelle. Nach § 27 Abs. 1 LDSG S-H umfasst der Auskunftsanspruch folgende Informationen: die zur Person der Betroffenen gespeicherten Daten, den Zweck und die Rechtsgrundlage der Speicherung, die Herkunft der Daten (§ 13 Abs. 1 S. 3 LDSG S-H), sowie die Empfänger von Übermittlungen (§ 14 Abs. 3 LDSG S-H, § 15 Abs. 2 S. 2 LDSG S-H), die Auftragnehmenden bei Datenverarbeitung im Auftrag, die Berichtigung, Löschung oder Sperrung von Daten, deren Verarbeitung nicht den gesetzlichen Bestimmungen entspricht, (insbesondere wenn diese Daten unvollständig oder unrichtig sind) und die Funktionsweise von automatisierten Verfahren.

[94] Simitis/*Dix*, BDSG, § 33 Rn. 36.
[95] Däubler/Klebe/Wedde/Weichert/*Däubler*, BDSG, § 33 Rn. 16.
[96] Simitis/*Dix*, BDSG, § 33 Rn. 38.
[97] Simitis/*Dix*, BDSG, § 33 Rn. 39.

Die Auskunft ist auf Antrag zu erteilen, d.h. im Unterschied zu § 26 LDSG S-H sind es hier die Betroffenen, die aktiv auf die datenverarbeitende Stell zukommen müssen, bzw. dürfen, um die Informationen zu erhalten. Es gibt gesetzlich keine formalen Anforderungen für die Antragstellung oder die Auskunftserteilung, d.h. beides wäre grds. mündlich oder per E-Mail möglich, soweit letztere vor Einsicht Dritter geschützt ist. Der Betroffene „soll" nach § 27 Abs. 1 S. 2 LDSG S-H die Art der personenbezogenen Daten, über die er Auskunft haben möchte, bezeichnen. Tut er dies nicht, empfiehlt es sich, um Konkretisierung zu bitten.[98] Im Rahmen des Tests dürfen jedoch auch alle vorgehaltenen Daten leicht zu beauskunften sein, so dass sich Rückfragen erübrigen.

Nach § 27 Abs. 1 S. 1 LDSG S-H besteht ein umfängliches Auskunftsrecht bzgl. folgender Informationen: die zur Person gespeicherten Daten, Zweck und Rechtsgrundlage der Speicherung, Herkunft der Daten (§ 13 Abs. 1 S. 3 LDSG S-H) und Empfänger von Übermittlungen (§§ 14 Abs. 3, 15 Abs. 2 S. 2 LDSG S-H), die Auftragnehmenden bei Datenverarbeitung im Auftrag, die Berichtigung, Löschung oder Sperrung von Daten, deren Verarbeitung nicht den gesetzlichen Bestimmungen entspricht, insbesondere wenn diese Daten unvollständig oder unrichtig sind und die Funktionsweise von automatisierten Verfahren die eingesetzt werden. Inhalt der zu erteilenden Auskunft wäre vorliegend also alle im Zeitpunkt des Auskunftsersuchens über die anfragende Person gespeicherten Daten, eine Kurzbeschreibung des Projekts und ein Verweis auf die Dienstvereinbarung, die Angabe der Projektpartner (unter Angabe eines Verantwortlichen und einer ladungsfähigen Anschrift), die aggregierte Daten von UKSH erhalten, ein Hinweis auf die auf Seiten des UKSH involvierten auftragnehmenden GmbHen und schließlich eine Kurzbeschreibung der eingesetzten Technik; hier insbesondere dass die Daten aus der Reaktion der Betroffenen auf Artefakte stammen. Soweit keine Daten (mehr) über den Betroffenen gespeichert sind, ist auch dies mitzuteilen.[99]

Ziel dieser Regelung – wie auch der Informationspflicht – ist es, Transparenz herzustellen. Die Betroffenen sollen in die Lage versetzt werden, zu wissen, was seine Kommunikationspartner über ihn wissen. Gleichzeitig soll auch die Rechtsdurchsetzung ermöglicht werden; d.h. es geht um die Möglichkeit Effektiv von seinen Rechten Gebrauch machen zu können.[100]

Nach § 27a LDSG S-H besteht ein besonderes Informationsrecht im Falle der unrechtmäßigen Kenntniserlangung von Daten durch Dritte. Die datenverarbeitende Stelle ist

[98] Däubler/Klebe/Wedde/Weichert/*Däubler*, BDSG, § 34 Rn. 24.
[99] Däubler/Klebe/Wedde/Weichert/*Däubler*, BDSG, § 34 Rn. 17.
[100] Däubler/Klebe/Wedde/Weichert/*Däubler*, BDSG, § 34 Rn. 1.

sowohl im Falle der unrechtmäßigen Übermittlung, als auch der sonstigen unrechtmäßigen Kenntniserlangung Dritter von Daten, die besonders geschützt sind, verpflichtet, unverzüglich die Betroffenen und das Unabhängige Landeszentrum für Datenschutz (in dessen Rolle als zuständige Aufsichtsbehörde) zu informieren, wenn schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen.

IV. Einwand, § 29 LDSG S-H

Nach § 29 Abs. 1 S. 1 LDSG S-H haben die Betroffenen haben das Recht, schriftlich unter Hinweis auf besondere persönliche Gründe Einwand gegen die Verarbeitung ihrer Daten allgemein oder gegen bestimmte Formen der Verarbeitung zu erheben. Sollte dies geschehen, ist gem. § 29 Abs.1 S. 2 LDSG S-H eine Abwägung vorzunehmen: Der Einwand ist begründet, wenn ein schutzwürdiges Interesse der oder des Betroffenen das öffentliche Interesse an der Datenverarbeitung im Einzelfall überwiegt. Im vorliegenden Fall sollten – unter Berücksichtigung der grundsätzlichen Wertung, dass niemand gegen oder ohne seinen Willen zum Forschungsobjekt gemacht werden soll (vgl. bereits zuvor) – die Daten des Betroffenen gelöscht werden. Eine Ausnahme vom Einwandsrecht nach § 29 Abs. 2 LDSG S-H greift nicht.

V. Berichtigung, Löschung und Sperrung, § 28 LDSG S-H

Die Betroffenen haben schließlich das Recht die Berichtigung, Löschung oder Sperrung ihrer personenbezogenen Daten zu verlangen.

Soweit Daten unrichtig sind, besteht ein Recht auf Berichtigung (§ 28 Abs. 1 LDSG S-H).

Der Anspruch auf Löschung besteht, wenn die Datenverarbeitung unzulässig ist (§ 28 Abs. 2 Nr. 1 LDSG S-H) oder wenn die Kenntnis der Daten für die datenverarbeitende Stelle zur Aufgabenerfüllung nicht mehr erforderlich ist (§ 28 Abs. 2 Nr. 2 LDSG S-H). „Löschen“ bedeutet das Unkenntlichmachen gespeicherter Daten. Der gespeicherte Inhalt darf endgültig nicht mehr lesbar sein.[101]

„Unzulässig“ ist eine Datenverarbeitung grundsätzlich, wenn kein Rechtsgrund (mehr) für sie besteht. Ein Beispiel ist etwa der begründete Einwand eines Betroffenen (siehe oben). Wann die Kenntnis der Daten zur Aufgabenerfüllung nicht mehr erforderlich ist, bestimmt sich in der Regel nach den bestehenden gesetzlichen Aufbewahrungsfristen.[102] Im Rahmen des Projektes werden die Rohdaten bzw. die an die Projektpartner herausgegebenen

[101] Däubler/Klebe/Wedde/Weichert/*Weichert*, BDSG, § 3 Rn. 44.
[102] Däubler/Klebe/Wedde/Weichert/*Däubler*, BDSG, § 35 Rn. 16.

pseudonymisierten Daten mit Abschluss des Projektes nicht mehr erforderlich in diesem Sinne sein und daher zu löschen. Zu diesem Zeitpunkt werden alle Messergebnisse in anonymisierte Statistiken überführt sein. Für die Dokumentation der Forschung ist dies ausreichend, sodass es der personenbezogenen Daten der Probanden nicht mehr bedarf. Dementsprechend wird in der Dienstvereinbarung die Löschung aller personenbezogenen Daten spätestens zum Ende der Projektlaufzeit festgeschrieben (§ 28 Abs. 2 S. 2 LDSG S-H).

An die Stelle des Rechts auf Löschung kann das Recht auf Sperrung treten. Sperren bedeutet das Untersagen weiterer Verarbeitung gespeicherter Daten (§ 2 Abs. 2 Nr. 4 LDSG S-H) und ist technisch oder textlich möglich;[103] d.h. etwa durch Ausblenden eines Datums für bestimmte Bearbeitungen oder Bearbeiter oder aber durch bloßes Hinzufügen eines Sperrvermerks.

§ 28 Abs. 3 LDSG S-H zählt die Fälle auf, in denen personenbezogene Daten (nur) zu sperren sind. Von Relevanz im hiesigen Zusammenhang könnte der Fall sein, dass die Richtigkeit der Daten vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit nachweisen lässt (Nr. 1), dass die Daten zur Aufgabenerfüllung nicht mehr erforderlich sind, Rechtsvorschriften jedoch die weitere Aufbewahrung anordnen (Nr. 2),[104] oder dass der Betroffene anstelle der Löschung die Sperrung verlangt (Nr. 3). Ebenso Sperrung statt Löschung kommt in Betracht, wenn die Betroffenen durch die Löschung in der Verfolgung ihrer Rechte oder in sonstigen schutzwürdigen Belangen beeinträchtigen würde (Nr. 4). Eine Sperrung bedeutet ein „relatives Nutzungsverbot“; abgesehen von einigen Ausnahmen ist keine Übermittlung oder Nutzung gestattet. Dementsprechend bestimmt § 28 Abs. 4 LDSG S-H dass gesperrte Daten grds. über die Speicherung hinaus ohne Einwilligung der Betroffenen nicht mehr weiterverarbeitet werden dürfen

Sollte es zu einer Berichtigung, Sperrung oder Löschung wegen Unzulässigkeit der Verarbeitung (d.h. im Projektkontext: Einwand eines Probanden) von Daten im UKSH kommen, muss es unverzüglich die Projektpartner, die die Daten pseudonymisiert erhalten haben hiervon – unter Wahrung der Pseudonymität – unterrichten (§ 28 Abs. 5 S. 1 LDSG S-H).

[103] Däubler/Klebe/Wedde/Weichert/*Weichert*, BDSG, § 3 Rn. 42.
[104] In Betracht kommt hier insbesondere die Aufbewahrung zu Beweiszwecken gegen schadensersatzrechtliche Ansprüche.

H. Übertragbarkeit auf andere Szenarien

Im Folgenden soll abschließend kurz auf die Übertragbarkeit der rechtlichen Erwägungen zur Testdurchführung auf andere Szenarien eingegangen werden.

I. Medizindaten

Gegenstand des Dokuments ist in erster Linie die datenschutzrechtliche Einordnung des Projekts ITS.APT. Die rechtliche Einschätzung ist dem Grunde nach auf jedes Szenario in einer öffentlichen Stelle des Landes Schleswig-Holstein übertragbar. Aus der Eigenschaft des UKSH als Gesundheitsdaten verarbeitende Stelle ergibt sich kaum eine Besonderheit, da im Rahmen der Tests keine Gesundheitsdaten verarbeitet werden. Allerdings wäre es in einer Stelle, die nicht Daten, die als „Geheimnisse“ im Sinne des § 203 StGB einzuordnen sind, mit ihren IT-System verarbeitet (vgl. oben D. II.), ein anderes Vorgehen möglich: Wenn ausgeschlossen werden kann, dass Daten in Sinne des § 203 StGB in der Stelle verarbeitet werden, kann ein ITS.APT-Tool potenziell auch direkt durch Externe in das System eingebracht werden und muss nicht durch die Verantwortlichen selbst, bzw. Gehilfen im Sinne des § 203 StGB eingesetzt werden.

II. Rechtsgrundlage

ITS.APT stützt seine Datenerhebung auf eine Dienstvereinbarung entsprechend dem Mitbestimmungsgesetz Schleswig-Holstein. Bei privatrechtlichen Unternehmen müsste aus arbeitsrechtlichen Gründen eine Betriebsvereinbarung entsprechend dem Betriebsverfassungsgesetz geschlossen werden. (Vgl. hierzu Dokument 2.1 – Arbeitsrechtliche Betrachtung.) Grundsätzlich kommt eine solche aber auch unter Geltung des BDSG als Rechtsgrundlage zur Datenerhebung in Betracht (§ 4 Abs. 1 BDSG).

Unter Geltung der DS-GVO ist die Rechtslage neu zu bewerten.

III. Technische Umsetzung

Hinsichtlich der technischen Umsetzung ist eine Übertragbarkeit auf andere Szenarien schwer einzuschätzen, da es hierfür maßgeblich auf das vorhandene IT-System ankommt.

Literaturverzeichnis

Brink, Stefan	Empfehlungen zur IuK-Nutzung am Arbeitsplatz, ZD 2015, 295-300 (Zitiert als: *Brink*, ZD 2015, 295)
Däubler, Wolfgang / Klebe, Thomas / Wedde, Peter / Weichert, Thilo	Bundesdatenschutzgesetz, 4. Auflage, Frankfurt 2013 (Zitiert als: Däubler/Klebe/Wedde/Weichert/*Bearbeiter*, BDSG, Rn. in §)
Geppert, Martin /Schütz, Raimund (Hrsg.)	Beck'scher TKG Kommentar, 4. Auflage, München 2013 (Zitiert als: BeckTKG/*Bearbeiter*, Rn. in §)
Gersdorf, Hubertus / Paal, Boris (Hrsg.)	Beck'scher Online-Kommentar Informations- und Medienrecht, 12. Edition, München 2016 (Zitiert als: BeckOK InfoMedienR/*Bearbeiter*, Gesetz, Rn. in §)
Kindhäuser, Urs / Neumann, Ulfrid / Paeffgen, Hans-Ullrich (Hrsg.)	Strafgesetzbuch, 4. Auflage, Nomos 2013 (Zitiert als: Kindhäuser/Neumann/Paeffgen/*Bearbeiter*, StGB, Rn. in §)
Lackner, Karl / Kühl, Kristian	Strafgesetzbuch Kommentar, 28. Auflage, München 2014 (Zitiert als: Lackner/Kühl/*Bearbeiter*, StGB, Rn. in §)
Maunz, Theodor / Dürig, Günter	Grundgesetz Kommentar, Stand: 75. Lieferung, München 2015 (Zitiert als: Maunz/Dürig/*Bearbeiter*, GG, Rn. in Art.)
Mayen, Thomas	Die Auswirkungen der Europäischen

	Datenschutzrichtlinie auf die Forschung in Deutschland, NvwZ 1997, 446-451 (Zitiert als: *Mayen*, NVwZ 1997, 446)
Roßnagel, Alexander	Das IT-Sicherheitsgesetz, DVBl. 2015, 1206-1212 (Zitiert als: *Roßnagel*, DVBl. 2015, 1206)
Schönke, Adolf / Schröder, Horst	Strafgesetzbuch Kommentar, 29. Auflage, München 2014 (Zitiert als: Schönke/Schröder/*Bearbeiter*, StGB, Rn. zu §)
Simitis, Spiros (Hrsg.)	Bundesdatenschutzgesetz, 8. Auflage, Baden-Baden 2014 (Zitiert als: Simitis/*Bearbeiter*, BDSG, Rn. zu §)
Spindler, Gerald / Schuster, Fabian	Recht der elektronischen Medien Kommentar, 3. Auflage, München 2015 (Zitiert als: Spindler/Schuster/*Bearbeiter*, Teil, Rn. in §)
Wolff, Heinrich Amadeus / Brink, Stefan (Hrsg.)	Beck'scher Online-Kommentar Datenschutzrecht, 15. Edition, München 2016 (zitiert als: BeckOK/*Verfasser*, Gesetz, Rn. in §)
Wybitul, Tim	Neue Spielregeln bei Betriebsvereinbarungen und Datenschutz – BAG schafft Klarheit zu Anforderungen an Umgang mit Arbeitnehmerdaten, NZA 2014, 225-232 (zitiert als: *Wybitul*, NZA 2014, 225)