datenschutz nord

Intevation GmbH
Februar 2010

Datenschutzrechtliche Verantwortlichkeiten für die Software „i-mpuls JMD“ im Rahmen der Jugendmigrationsdienste

(„Programm 18“ im Kinder- und Jugendplan des Bundes (KJP),„Integration junger Menschen mit Migrationshintergrund“)

1. Einführung

Nachfolgend sollen die datenschutzrechtlichen Verantwortlichkeiten der am Projekt „I-mpuls JMD“ Beteiligten, also den Jugendmigrationsdiensten, den Trägergruppen bzw. Bundestutoren sowie dem DLR bzw. dem Bundesministerium für Familie, Senioren, Frauen und Jugend (BMFSFJ) dargestellt und erläutert werden. Ziel ist es, anhand einer klaren Zuteilung der Verantwortlichkeiten die datenschutzrechtlichen Rahmenbedingungen für die jeweiligen Datenverarbeitungen zu bestimmen und die wiederum hieraus resultierenden Aufgaben zu definieren.

Hinzuweisen ist dabei vorab darauf, dass die nachfolgenden Ausführungen eine rein datenschutzrechtliche Bewertung darstellen, förderrechtliche Aspekte werden vorliegend nicht dargestellt bzw. nur soweit berücksichtigt, wie dies für das datenschutzrechtliche Verständnis erforderlich ist.

2. Jugendmigrationsdienste

2.1 Rechtsform , anwendbares Recht und Verantwortlichkeit

Die Stellen der Jugendmigrationsdienste vor Ort sind die aus datenschutzrechtlicher Sicht zentralen Akteure. Sie sind in unterschiedlichsten Rechtsformen organisiert, zum Teil als gemeinnützige Gesellschaften mit beschränkter Haftung (gGmbH), als privatrechtlich organisierte eingetragene Vereine oder als (z.T. juristisch und wirtschaftlich eigenständige) Abteilungen der beteiligten Trägergruppen.

Unabhängig von der im Einzelfall gewählten Rechtsform ist auf die mit dem Verfahren i-mpuls durchgeführte Datenverarbeitung[1] dieser zentralen Akteure stets das Bundesdatenschutzgesetz (BDSG) anwendbar. Diese Anwendbarkeit ergibt sich mittelbar aus dem Förderrecht: Rechtsgrundlage der Zuwendungen an die Jugendmigrationsdienste bzw. der Trägergruppen ist die zu § 44 BHO erlassene KJP-

[1] Abhängig von der konkreten Rechts- bzw. Organisationsform bleiben für die sonstigen datenschutzrelevanten Tätigkeiten der JMDe die jeweiligen Landesdatenschutzgesetze (bei öffentlichen Stellen) bzw. kirchlichen Datenschutzgesetze (bei kirchlichen Stellen) anwendbar.

Richtlinie, die u.a. die allgemeinen Fördergrundsätze enthält. Hiernach erfolgt die Förderung durch Zuwendungen an die Erstzuwendungsempfänger (Trägergruppen) mit der Möglichkeit der Weiterleitung an Letztzuwendungsempfänger (JMDe). Seitens der Zuwendungsempfänger besteht allerdings kein (Rechts-)Anspruch auf die Zuwendungen, zudem sind die Zuwendungsempfänger auch nicht formell beliehen. Aus diesem Grund erfüllen sie mit ihrer Tätigkeit keine öffentlichen Aufgaben im datenschutzrechtlichen Sinne – wenngleich die Tätigkeiten fraglos der Erfüllung (wichtiger) öffentlicher Interessen dienen.

Eine Datenverarbeitung ist gem. § 4 Abs. 1 BDSG nur zulässig, wenn eine Rechtsvorschrift sie erlaubt oder eine Einwilligung des Betroffenen vorliegt.

Da, wie zuvor erwähnt, kein Rechtsanspruch auf die hier relevanten Zuwendungen besteht und die Förderrichtlinien auch keine Rechtsvorschrift mit Außenwirkung im datenschutzrechtlichen Verständnis darstellen, mangelt es für die relevante Datenverarbeitung an einer solchen Rechtsvorschrift. Aus diesem Grund müssen die Teilnehmer eine detaillierte Einwilligungserklärung abgeben, nur so kann eine datenschutzrechtlich tragbare Rechtsgrundlage geschaffen werden (vgl. die Anforderungen an eine wirksame Einwilligungserklärung im **Anhang**). Das DLR als Projektträger gibt diese Einwilligungserklärung als Empfehlung für die JMDe bzw. deren Trägergruppen vor.

Die Jugendmigrationsdienste sind vorliegend auch (jeweils) datenschutzrechtlich verantwortliche Stelle i.S.d. § 3 Abs. 7 Bundesdatenschutzgesetz (BDSG):

Die Erhebung und Verarbeitung der personenbezogenen Daten der Betroffenen erfolgt zu eigenen Zwecken, nämlich zur Verbesserung der Integrationschancen durch sprachliche, schulische und soziale Integration. Natürlich werden diese Ziele und Zwecke mit den Trägergruppen gemeinsam vereinbart und kontinuierlich optimiert. Gleichwohl sind die jeweiligen Jugendmigrationsdienste diejenigen Stellen vor Ort, die das CaseManagement durchführen und hierfür die personenbezogenen Daten verarbeiten. Damit sind sie alleinige Adressaten datenschutzrechtlicher Pflichten und Rechte – sowohl derjenigen nach dem BDSG, als auch derjenigen nach anderen einschlägigen, z.T. spezielleren Rechtsvorschriften.

Soweit sich die verantwortlichen Stellen bei der Datenverarbeitung der Hilfe eines oder mehrerer Auftragnehmer bedienen, verbleibt die Verantwortlichkeit gleichwohl bei ihnen, vgl. § 11 BDSG. Als „Ausgleich“ hierfür kann und muss die verantwortliche Stelle die Rahmenbedingungen für die Auftragsdatenverarbeitung detailliert und verbindlich, d.h. im Zweifel auch mit Haftungstatbeständen, schriftlich regeln (Näheres zur Auftragsdatenverarbeitung vgl. unten Ziff. 3)

2.2 Datenverarbeitungen

Die Jugendmigrationsdienste als verantwortliche Stellen erheben, speichern und verarbeiten personenbezogene Daten der Jugendlichen. Dies erfolgt automatisiert in Form einer elektronischen Fallakte (datenbankgestützte Client-Server-Anwendung I-mpuls). Mithilfe der Anwendung i-mpuls werden personenbezogene Daten für Auswertungszwecke auch an das PT-DLR übermittelt (auf den sog. „Auswertungsserver“). Der übermittelte Datensatz wird hierbei allerdings gekürzt um den Namen, die Adresse, Geburtsdatum sowie weitere Textfelder mit potenziellem Personen-

bezug, so dass im Ergebnis nur noch ein anonymisiertes Datum verbleibt (zur rechtlichen Bewertung vgl. Ziff. 4.3.2). Zugriff auf die anonymisierten Daten des Auswertungsservers haben auch die Trägergruppen.

Eine „Löschung" der Daten erfolgt entweder aufgrund eines Widerrufs der Einwilligungserklärung des Jugendlichen oder automatisch nach einer festgelegten Frist nach Beendigung der Maßnahme. Um die Statistiken nicht zu verfälschen, werden in diesem Fall die Daten nicht komplett gelöscht, sondern – wie zuvor beschrieben – anonymisiert. Soweit Daten anonymisiert, d.h. nicht mehr auf eine Person zurückführbar sind, können sie ohne Löschfristen gespeichert bleiben.

2.3 Aufgaben der verantwortlichen Stelle(n)

Wie unter Ziff. 2.1 bereits angedeutet, sind die jeweiligen Jugendmigrationsdienste als verantwortliche Stellen für das Verfahren i-mpuls Adressaten der damit verbundenen datenschutzrechtlichen Pflichten und Rechte. Hiervon unberührt bleiben die weiteren datenschutzrechtlichten Zuständigkeiten der Zentralen der Trägergruppen, diese werden von den betrieblichen Beauftragten für den Datenschutz wahrgenommen.

Als verantwortliche Stellen für die Anwendung i-mpuls sind die Jugendmigrationsdienste somit dafür verantwortlich dass

- --- eine wirksame Rechtsgrundlage für die Datenverarbeitung existiert, § 4 Abs. 1, § 4a BDSG – hier die Einwilligung
- --- die personenbezogenen Daten korrekt verarbeitet werden bzw. aktuell sind
- --- die Zweckbindung des § 4 Abs. 3 Nr. 2 BDSG beachtet wird
- --- bei Vorliegen der entsprechenden Voraussetzungen entweder ein betrieblicher Datenschutzbeauftragter bestellt ist (mit entsprechender Fachkunde und Zuverlässigkeit, § 4f BDSG) oder die Verfahren der Aufsichtsbehörde zu melden sind, § 4d Abs. 3 BDSG
- --- ein aktuelles Verfahrensverzeichnis vorliegt, § 4g Abs. 2 i.V.m. § 4e BDSG
- --- die Mitarbeiter über datenschutzrechtliche Anforderungen informiert bzw. geschult sind, § 4g Abs. 1 Nr. 2 BDSG
- --- die Betroffenen ihre Auskunfts-, Berichtigungs- und Löschrechte geltend machen können, §§ 33-35 BDSG
- --- sie selbst und/oder Auftragnehmer die technisch-organisatorischen Sicherheitsmaßnahmen für die automatisierte Datenverarbeitung gem. § 9 BDSG + Anlage zu § 9 vorhalten
- --- Entbindungen von der Schweigepflicht vorliegen, bevor Geheimnisse im Sinne des § 203 StGB Dritten offenbart werden

Mit dieser Verantwortlichkeit ist allerdings nur ein Teil der datenschutzrechtlichen Rahmenbedingungen des Betriebs von i-mpuls beleuchtet. Hinzu kommt die Rolle des PT-DLR als Betreiber der Client-Server-Anwendung:

3. Auftragsdatenverarbeitung durch das PT-DLR

Unter Ziff. 2.1 am Ende wurde bereits kurz erwähnt, dass die JMD auch dann verantwortlich bleiben für die Datenverarbeitung, wenn sie Auftragnehmer hierfür einsetzen bzw. sich Dritter bei der Datenverarbeitung bedienen. Dies gilt auch für den Einsatz von (Hosting-)Software, mit der die Daten der Teilnehmer automatisiert verarbeitet werden. Unabhängig davon, ob lokale Software oder netzwerkgestützte Client-Server-Anwendungen eingesetzt werden, die von einem Dienstleister – hier dem PT-DLR bzw. Unterauftragnehmern– zur Verfügung gestellt werden, bleibt der JMD datenschutzrechtlich verantwortlich.

Es ergibt sich damit rechtlich ein vom Tatsächlichen abweichendes Bild: Die Jugendmigrationsdienste sind und bleiben verantwortliche Stellen und damit auch zuständig für die Nutzung der Anwendungen, mit denen sie die pb Daten der Teilnehmer verwalten – jedoch nur soweit sie die Daten der Teilnehmer für ihre Zwecke verarbeiten (die Verantwortlichkeit ginge auf das PT-DLR über, sobald diese die Daten für eigene Zwecke verarbeitete, z.B. eine personenbezogene(!) Auswertung der Daten vornähme).

Gem. § 11 BDSG müssen sie als Auftraggeber dem Auftragnehmer (PT-DLR) schriftlich vorgeben, wie die Daten zu verarbeiten sind bzw. welche technisch-organisatorischen Sicherheitsmaßnahmen gem. § 9 nebst Anlage BDSG einzuhalten sind. Im Tatsächlichen arbeiten die Akteure in der Regel, so auch hier, genau gegensätzlich: Der technische Dienstleister hält Sicherheitsmaßnahmen auf aktuellem Stand der Technik (Authentisierung, Sicherung, Backup, Verschlüsselung etc.) und in der Regel auch entsprechende Software vor und bietet diese dem Auftraggeber an.

Um die Datenverarbeitung beim PT-DLR jedoch trotz der fehlenden direkten Einflussmöglichkeit der JMDe kontrollieren zu können, ist es erforderlich, die Auftragsdatenverarbeitung mit dem PT-DLR schriftlich im Detail zu vereinbaren. Inhalte dieser Vereinbarung müssen aus datenschutzrechtlicher Sicht sein

- Gegenstand und Dauer des Auftrags (eine genaue Beschreibung der IT-Dienstleistungen des PT-DLR für die JMDe),
- der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
- eine Zusicherung, dass alle Mitarbeiter des PT-DLR, die mit der DV in Berührung kommen, auf das Datengeheimnis nach § 5 BDSG verpflichtet sind,
- die Berichtigung, Löschung und Sperrung von Daten sowie die Rückgabe von Datenträgern und die Löschung nach Beendigung des Auftrags,
- die Festlegung etwaiger Unterauftragsverhältnisse (z.B. Provider),
- der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem PT-DLR vorbehält,
- die Kontrollrechte der Auftraggeber und die entsprechenden Duldungs- und Mitwirkungspflichten des PT-DLR,
- die Verpflichtung, dass der Auftragnehmer bei unzulässigen Weisungen des JMD diesen darauf aufmerksam macht,

--- eine möglichst detaillierte Auflistung der technisch-organisatorischen Sicherheitsmaßnahmen, die sich das PT-DLR verpflichtet, einzuhalten

Die vorgenannten Pflichten orientieren sich an der Neufassung des § 11 BDSG vom 1.9.2009. Die hierin vom Bundesgesetzgeber geregelten Anforderungen gehen allerdings z.Zt. zum Teil über diejenigen hinaus, die die jeweiligen Landesdatenschutzgesetze regeln. Um aber eine bundesweit einheitliche Regelung in Form eines Mustervertrages treffen zu können, der für JMDe öffentlicher, nicht-öffentlicher und kirchlicher Träger Anwendung finden kann, enthält der Mustervertrag im Sinne eines argumentum a maiore ad minus sämtliche Rechte und Pflichten des § 11 BDSG unter Berücksichtigung insbesondere auch der technisch-organisatorischen Sicherheitsmaßnahmen.

4. Projektträger (PT-DLR)

4.1 Rechtsform

Das Deutsche Zentrum für Luft- und Raumfahrt ist als privatrechtlicher (eingetragener) Verein organisiert, nicht beliehen und daher nicht-öffentliche Stelle i.S.d. BDSG. Auch für diesen gelten daher sämtliche Regelungen des Bundesdatenschutzgesetzes.

4.2 Geplante Datenverarbeitungen

Dem PT-DLR obliegt die Auswertung der bei den Jugendmigrationsdiensten erhobenen und gespeicherten personenbezogenen Daten: Entsprechend den Vorgaben der Förderrichtlinie sollen u.a. ausgewertet werden

--- wie viele Jugendliche in den Jugendmigrationsdiensten beraten wurden
--- welche Merkmale die Jugendlichen aufweisen
--- wie lange das Case-Management durchschnittlich dauert
--- wie hoch die Integrationsquoten sind
--- sowie weitere Auswertungen.

Festzustellen ist damit zunächst, dass mit dieser Datenverarbeitung ein weiterer, über den ursprünglichen Zweck hinausgehender Zweck verfolgt wird, als mit der ursprünglichen Erhebung und Verarbeitung durch die Jugendmigrationsdienste: Wird dort primär die Integration der betroffenen Jugendlichen bezweckt, ist es Aufgabe des PT-DLR, Informationen für das Monitoring des Programms anhand anonymisierter Einzelfalldaten zu erstellen. Die für diesen Zweck erforderliche Übermittlung[2] der Daten als auch die damit verbundene Zweckänderung wäre auf gesetzlicher Grundlage nur zulässig, wenn für die Übermittlung eine gesetzliche Grundlage existiert. Da vorliegend jedoch eine Einwilligung als Rechtsgrundlage verwendet wird, muss die Übermittlung bereits explizit in der Einwilligung berücksichtigt werden, so dass für den Einwilligenden nachvollziehbar ist, dass seine

[2] Ob die Daten an das PT-DLR tatsächlich aktiv „übermittelt“ werden, oder ob das PT-DLR einen Zugriff auf den (reduzierten) Datensatz über ein Netzwerk erhält, ist rechtlich unerheblich, da gem. § 3 Abs. 3 Nr. 4b BDSG eine Übermittlung rechtlich auch dann vorliegt, wenn einem Dritten ein Zugriff auf die Daten gewährt wird.

personenbezogenen Daten nicht nur von einer, sondern von mehreren verantwortlichen Stellen genutzt werden. Diese Anforderung ist in dem vorliegenden Entwurf der Einwilligungserklärung umgesetzt worden.

4.3 Datenschutzrechtliche Bewertung

4.3.1 Verantwortlichkeit

Aus der Tatsache, dass das PT-DLR mit der Verarbeitung der übermittelten Daten eigene Zwecke verfolgt, die mit denjenigen der Jugendmigrationsdienste nicht identisch sind, folgt, dass es für diesen Teil der Datenverarbeitung selbst verantwortliche Stelle ist (vgl. dazu schon oben Ziff. 2.4). Hieraus wäre nun zunächst ohne Weiteres der Schluss zu ziehen, dass die oben unter Ziff. 2.3 genannten rechtlichen Rahmenbedingungen auch für das PT-DLR gelten, soweit es personenbezogene Daten der Betroffenen verarbeitet. Aufgrund der geplanten Verkürzung des Datensatzes um bestimmte Datenfelder wie Name und Adresse stellt sich jedoch die Frage, ob der auf diese Weise übermittelte Datensatz überhaupt noch personenbezogen i.S.d. § 3 Abs. 1 BDSG ist, d.h. ob mit dem verbliebenen Datensatz überhaupt noch eine bestimmte oder bestimmbare natürliche Person im Sinne der gesetzlichen Definition als Betroffener identifizierbar ist. Lägen mit dem verbliebenen Datensatz nur noch anonymisierte Daten vor, wäre das BDSG mangels personenbezogener Daten nicht (mehr) anwendbar.

4.3.2 Anonymisierung / Pseudonymisierung

Zum derzeitigen Stand ist geplant, bei der Übermittlung des Datensatzes an das PT-DLR sowohl den Namen, die Adresse sowie das Geburtsdatum des Betroffenen zu unterdrücken bzw. aus dem Datensatz zu entfernen.

Ein Anonymisieren liegt gem. der Legaldefinition des § 3 Abs. 6 BDSG vor, wenn

> personenbezogene Daten derart verändert werden, dass die Einzelangabe 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.

Vor dem Hintergrund dieser Definition läge mit der Entfernung der o.g. Angaben auf den ersten Blick eine Anonymisierung vor, da ohne Namen, Adresse und Geburtsdatum eine Zuordnung zu einer bestimmten Person nicht mehr möglich scheint, zumindest nicht für den Kreis der Empfänger bzw. derer, die mit den (reduzierten) Daten arbeiten.

Das Datenschutzgesetz stellt jedoch an die Anonymisierung hohe Anforderungen, da hiermit die Anwendbarkeit des gesamten Gesetzes (bzw. datenschutzrechtlicher Normen überhaupt) steht und fällt. Ein anonymisierter Datensatz liegt z.B. nicht vor, wenn der reduzierte Datensatz wieder mit dem ursprünglichen zusammengeführt werden kann, d.h. wenn die Identifikatoren lediglich getrennt von den sonstigen

Merkmalen gespeichert werden[3] und eine jederzeitige Rückführung möglich ist. Folgende Möglichkeiten der Anonymisierung erfüllen hingegen die gesetzlichen Voraussetzungen[4]:

- **Löschung** der expliziten bzw. direkten Identifikationsmerkmale (Name, Anschrift etc.)
- **Merkmalsaggregierung** (die Ersetzung von Angaben durch Ersatzangaben (statt Geburtsjahr die beschriebenen „Altersgrenzen“ bzw. „Altersbereiche“), Ersetzung quantitativer Merkmale (z.B. Größe, Einkommen, Alter) durch größere Größenklassen (z.B. Einkommen über 2.500,- Euro)
- Einbringung von **Zufallsfehlern** in den Datenbestand („Kontamination“), z.B. durch Vertauschen von Merkmalen im Sinne einer Zuordnung von vorhandenen Merkmalen zu anderen Bezugspersonen, soweit dies unter Berücksichtigung der Auswertungsziele möglich ist

Erforderlich ist in jedem Fall, dass der anonymisierte Datensatz von dem ursprünglichen (personenbezogenen) Datensatz getrennt vorliegt, dass es sich bei dem von PT-DLR verarbeiteten Datensatz also um einen separaten Datensatz handelt. Dies muss beim Betrieb von i-mpuls berücksichtigt werden.

5. Die datenschutzrechtliche Rolle der Trägergruppen

Die in diesem Verfahren als Erstzuwendungsempfänger beteiligten Trägergruppen sollen nach dem jetzigen Stand Zugriff auf die – jeweils ihren Jugendmigrationsdiensten zuzuordnenden - anonymisierten Daten des Auswertungsservers erhalten. Mit dieser Zugriffsmöglichkeit bleibt eine „Nachverfolgbarkeit“ der Tätigkeiten „ihrer“ Jugendmigrationsdienste und damit auch die Möglichkeit eines Verwendungsnachweises und der Erfolgskontrolle erhalten, ohne dass hierdurch jedoch zusätzliche datenschutzrechtliche Fragen aufgeworfen werfen müssen. Denn bei der Zugriffsmöglichkeit auf (anonymisierte) Fallakten handelt es sich datenschutzrechtlich nicht um eine Datenübermittlung, die wiederum nur auf gesetzlicher Grundlage zulässig wäre. Vielmehr liegt damit eine Datenverarbeitung vor, die wegen der zuvor erfolgten Anonymisierung zulässig ist.

[3] vgl. Simitis, § 3 BDSG, Rdn. 200

[4] vgl. Simitis, a.a.O, Rdn. 206 - 2111

Anhang:

Anforderungen an eine wirksame Einwilligung gem. § 4a BDSG

Da mit einer Einwilligungserklärung gem. § 4a Abs. 1 BDSG eine eigene Rechtsgrundlage für eine Datenverarbeitung geschaffen wird, die ansonsten rechtswidrig wäre, stellt das BDSG, aber auch die Landes- und Kirchendatenschutzrechte an die Wirksamkeit und Reichweite solcher Einwilligungen hohe Anforderungen. Einwilligungen bedürfen daher zur Wirksamkeit

- --- der Freiwilligkeit der Abgabe der Erklärung
- --- einer detaillierten Information des Betroffenen über die zu verarbeitenden Daten, den Zweck (und die Dauer) der Erhebung, Verarbeitung oder Nutzung sowie
- --- eines Hinweises auf die Folgen der Verweigerung der Einwilligung
- --- einer schriftlichen Erklärung

Soweit besondere Arten personenbezogener Daten gem. § 3 Abs. 9 BDSG erhoben, verarbeitet oder genutzt werden sollen, muss sich die Einwilligung darüber hinaus **explizit** auch hierauf beziehen (vgl. dazu unten Ziff. 3 am Ende). Schließlich ist hinsichtlich der Wirksamkeit darauf hinzuweisen, dass eine Einwilligungserklärung gem. § 4a BDSG keine Willenserklärung gem. §§ 104 ff BGB darstellt, so dass für eine wirksame Abgabe **keine** Geschäftsfähigkeit (18 Jahre-Grenze) erforderlich ist. Vielmehr kann eine wirksame Einwilligung auch durch Minderjährige abgegeben werden, wenn diese die für die Tragweite der Erklärung erforderlich Einsichtsfähigkeit haben. Diese wiederum hängt ab vom konkreten Verwendungszusammenhang, kann also nicht generell an einer bestimmten Altersgrenze festgemacht werden. Es ist aber davon auszugehen, dass eine solche Einsichtsfähigkeit mit 16 Jahren vorliegt.

Grenzen der Einwilligungserklärung

Wie im Dokument ausgeführt, ermöglicht die wirksame Einwilligungserklärung grundsätzlich eine umfangreiche Datenerhebung, Verarbeitung und auch Übermittlung der personenbezogenen Daten. Die Grenze dieser Rechtsgrundlage ist jedoch dort erreicht, wo Daten Dritter erhoben werden sollen (z.B. personenbezogene Daten der Eltern oder sonstiger Erziehungsberechtigter des Betroffenen) bzw. wo Daten von Dritten eingeholt werden, ohne dass der Betroffene hierbei im Vorhinein, d.h. zum Zeitpunkt der Abgabe der Einwilligungserklärung, übersehen kann, welche Daten zu welchen Zwecken bei Dritten erhoben und verarbeitet werden. Grenzen der Einwilligungserklärung ergeben sich weiterhin dergestalt, dass sich die Einwilligung stets nur auf personenbezogene Daten beziehen kann, die direkt vom Betroffenen stammen. Informationen hingegen, die erst durch eine Bewertung bzw. Auswertung von personenbezogenen Daten entstehen (z.B. Beurteilungen der intellektuellen, sprachlichen oder handwerklichen Leistungsfähigkeit – „subjektive“ Daten), können von einer Einwilligung nicht (mehr) umfasst sein, wenn der Betroffene von dieser bewertenden Datenverarbeitung keine Kenntnis erhält.

Schließlich muss sichergestellt sein, dass ein Widerruf der Einwilligung technisch auch so umgesetzt werden kann, dass die personenbezogenen Daten bei Ausübung des Widerrufs auch gelöscht bzw. anonymisiert werden können.