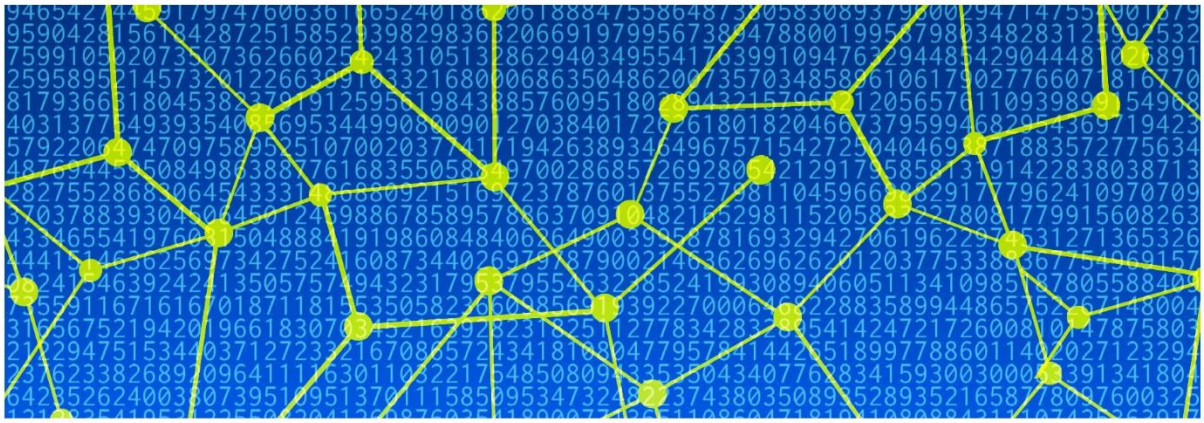

EUROPEAN DATA PROTECTION SUPERVISOR

Stellungnahme 9/2016

Stellungnahme des EDSB zu Systemen für das *Personal Information Management (PIM)*

Hin zu einer intensiveren Einbindung der Nutzer in das Management und die Verarbeitung personenbezogener Daten

20. Oktober 2016

Der Europäische Datenschutzbeauftragte (EDSB) ist eine unabhängige Einrichtung der EU und hat nach Artikel 41 Absatz 2 der Verordnung (EG) Nr. 45/2001 „im Hinblick auf die Verarbeitung personenbezogener Daten (...) sicherzustellen, dass die Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere ihr Recht auf Privatsphäre, von den Organen und Einrichtungen der Gemeinschaft geachtet werden"; er ist „für die Beratung der Organe und Einrichtungen der Gemeinschaft und der betroffenen Personen in allen die Verarbeitung personenbezogener Daten betreffenden Angelegenheiten" zuständig. Gemäß Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 ist die Kommission zur Konsultation des EDSB verpflichtet, „wenn [sie] einen Vorschlag für Rechtsvorschriften bezüglich des Schutzes der Rechte und Freiheiten von Personen bei der Verarbeitung personenbezogener Daten annimmt".

Er wurde zusammen mit dem Stellvertretenden Datenschutzbeauftragten im Dezember 2014 ernannt und spezifisch mit einem konstruktiven und proaktiven Vorgehen beauftragt. In der im März 2015 veröffentlichten Fünf-Jahres-Strategie legt der EDSB dar, wie er diesen Auftrag auf verantwortungsvolle Weise zu erfüllen gedenkt.

In dieser Stellungnahme geht es um den Auftrag des EDSB, die EU-Organe bezüglich der Datenschutzimplikationen ihrer Politiken zu beraten und eine verantwortliche Politikgestaltung zu fördern, im Einklang mit Maßnahme 9 der Strategie des EDSB: „Förderung einer verantwortungsvollen und fundierten politischen Entscheidungsfindung". Nach Auffassung des EDSB sollte die neu entstehende Landschaft von Systemen für das Personal Information Management (PIMS), mit denen natürlichen Personen und Verbrauchern die Kontrolle über ihre personenbezogenen Daten zurückgegeben werden soll, daraufhin betrachtet werden, dass sie einen Beitrag zu einer nachhaltigen und ethisch verantwortlichen Verwendung von Big Data und zu einer wirksamen Umsetzung der Grundsätze der kürzlich verabschiedeten Datenschutz-Grundverordnung (DSGV) leisten kann.

Zusammenfassung

Diese Stellungnahme untersucht das Konzept, das hinter Technologien und Ökosystemen steht, mit denen Menschen in die Lage versetzt werden sollen, die Weitergabe ihrer personenbezogenen Daten zu kontrollieren („Personal Information Management-Systeme“ oder kurz „PIMS“).

Uns schwebt die Schaffung einer neuen Realität vor, in der Menschen ihre Online-Identität managen und kontrollieren können. Unser Ziel ist es, das derzeitige anbieterzentrierte System in ein menschenzentriertes System umzuwandeln, in dem natürliche Personen vor der unrechtmäßigen Verarbeitung ihrer Daten und vor in ihre Privatsphäre eindringenden Techniken des Nachverfolgens von Verhalten und der Profilerstellung (*Tracking and Profiling*) geschützt werden, mit denen zentrale Grundsätze des Datenschutzes umgangen werden sollen.

Unterstützt wird diese neue Realität durch den modernisierten EU-Regelungsrahmen und die Möglichkeiten, die sich aus entschlossener, gemeinschaftlicher Durchsetzung durch alle einschlägigen Aufsichts-und Regulierungsbehörden ergeben.

Die vor kurzem verabschiedete Datenschutz-Grundverordnung (DSGV) stärkt und modernisiert den rechtlichen Rahmen, damit er im Zeitalter von Big Data wirksam bleibt; hierzu muss das Vertrauen des Einzelnen in Online-Aktivitäten und in den digitalen Binnenmarkt gestärkt werden. Die neuen Vorschriften, unter anderem zu mehr Transparenz und starken Rechten auf Auskunft und Datenübertragbarkeit, können als Voraussetzung dafür dienen, dass Benutzer mehr Kontrolle über ihre Daten haben, und sie können ferner zur Entwicklung effizienterer Märkte für personenbezogene Daten zugunsten von Verbrauchern und Unternehmen beitragen.

Erst unlängst haben wir eine Stellungnahme zur wirksamen Durchsetzung von Grundrechten im Zeitalter von Big Data herausgegeben. Darin werden die bestehenden Marktbedingungen und Geschäftspraktiken hervorgehoben, die einer wirksamen Ausübung der Rechte natürlicher Personen auf den Schutz ihrer personenbezogenen Daten und anderer Grundrechte im Wege stehen, und wird gefordert, die abgestimmte und kohärente Durchsetzung von Wettbewerbs-, Verbraucherschutz- und Datenschutzrecht zu intensivieren. Wir hoffen, dass sich mit einer solchen intensiveren Durchsetzung Marktbedingungen herstellen lassen, in denen datenschutzfreundliche Dienste gedeihen können. Der in dieser Stellungnahme verfolgte Ansatz zielt auf die Stärkung von Grundrechten in unserer digitalen Welt und gleichzeitig auf die Eröffnung neuer Chancen für Unternehmen ab, auf gegenseitigem Vertrauen beruhende innovative, auf personenbezogenen Daten fußende Dienste zu entwickeln. PIMS versprechen, nicht nur ein neue technische Architektur und Organisation für das Datenmanagement zu bieten, sondern auch Rahmen, in denen Vertrauen entstehen kann und daraus wiederum alternative Geschäftsmodelle für die Erhebung und Verarbeitung personenbezogener Daten im Zeitalter von Big Data auf eine Weise werden können, die dem europäischen Datenschutzrecht besser Rechnung tragen.

In dieser Stellungnahme beschreiben wir kurz, was PIMS sind, welche Probleme sie lösen sollen und wie das geschehen soll. Im Anschluss daran gehen wir der Frage nach, wie sie zu einem besseren Schutz personenbezogener Daten beitragen können und vor welchen Herausforderungen sie dabei stehen. Abschließend befassen wir uns mit künftigen Möglichkeiten, die von ihnen gebotenen Chancen sinnvoll zu nutzen. Damit neue Geschäftsmodelle für den Datenschutz Erfolg haben, sind möglicherweise weitere Anreize für die Dienstanbieter erforderlich, die diese anbieten. So sollte insbesondere in Erfahrung

gebracht werden, welche politischen Initiativen Verantwortliche dazu motivieren könnten, diese Art der Datenbereitstellung zu akzeptieren. Ferner könnte eine Initiative öffentlicher Dienststellen, PIMS als Datenquelle an Stelle einer direkten Datenerhebung zu akzeptieren, die kritische Masse für eine Akzeptanz von PIMS vergrößern.

Die neu entstehende Landschaft von PIMS, mit denen natürlichen Personen und Verbrauchern die Kontrolle über ihre personenbezogenen Daten zurückgegeben werden soll, verdient Betrachtung, Unterstützung und weitere Erforschung im Hinblick darauf, dass sie einen Beitrag zu einer nachhaltigen und ethisch verantwortlichen Verwendung von Big Data und zu einer wirksamen Umsetzung der Grundsätze des kürzlich verabschiedeten DSGV leisten kann.

INHALT

1. PIMS: IST DIE WEITERGABE VON DATEN MIT DER WEITERGABE VON VORTEILEN GLEICHZUSETZEN? 6

2. MODELLE UND MERKMALE NEU ENTSTEHENDER PIMS 7

2.1. ARCHITEKTUR UND TECHNOLOGIE 7

2.2. HAUPTMERKMALE, DIE PERSONEN DIE KONTROLLE ÜBER IHRE PERSONENBEZOGENEN DATEN ERLEICHTERN 9

2.3. POLITISCHER RAHMEN UND GESCHÄFTSMODELLE FÜR PIMS 9

3. WIE KÖNNEN PIMS DIE DATENSCHUTZGRUNDSÄTZE UNTERSTÜTZEN? 10

3.1. WIRKSAMES EINWILLIGUNGSMANAGMENT FÜR EINE ECHTE NUTZERKONTROLLE UND DIE VERWENDUNG AUTOMATISIERTER MECHANISMEN 10

3.2. NUTZER MIT KONTROLLE, RECHT AUF AUSKUNFT UND AUF BERICHTIGUNG, RECHT AUF DATENPORTABLITÄT, DATENQUALITÄT 11

3.3. DATENSCHUTZ DURCH TECHNIK UND DATENSCHUTZFREUNDLICHE VOREINSTELLUNGEN, INTEROPERABILITÄT 12

3.4. TECHNISCHE MITTEL ZUR EINSCHRÄNKUNG DER WEITERVERWENDUNG PERSONENBEZOGENER DATEN 12

3.5. TRANSPARENZ UND RÜCKVERFOLGBARKEIT 13

3.6. DATENSICHERHEIT 13

3.7. ÜBERMITTLUNGEN PERSONENBEZOGENER DATEN 14

3.8. FUNKTION DES VERANTWORTLICHEN UND HAFTUNG 14

3.9. SUCHE NACH EINEM NACHHALTIGEN GESCHÄFTSMODELL IM INTERESSE DER BETROFFENEN PERSONEN 15

3.10. ES GEHT MEHR UM DIE „GENEHMIGUNG DER VERWENDUNG“ PERSONENBEZOGENER DATEN ALS UM DEREN „VERKAUF“ 16

4. SCHLUSSFOLGERUNGEN UND NÄCHSTE SCHRITTE 16

4.1 HIN ZU EINER VOLLSTÄNDIGEN ANWENDUNG DER DSGV 16

4.2 UNTERSTÜTZUNG VON PIMS UND DER IHNEN ZUGRUNDE LIEGENDEN TECHNOLOGIE FÜR WIRKSAMEN DATENSCHUTZ 17

4.3 WIE BRINGT DER EDSB DIESE DEBATTE VORAN? 18

Endnoten 19

1. PIMS: IST DIE WEITERGABE VON DATEN MIT DER WEITERGABE VON VORTEILEN GLEICHZUSETZEN?

1 Die derzeitigen Bedingungen für die Verarbeitung personenbezogener Daten sind häufig den Personen gegenüber unfair, deren Daten verarbeitet werden. Rechtliche Lage und technische Instrumente erschweren natürlichen Personen die Ausübung ihrer Rechte und erlauben den Verantwortlichen, ihre Haftung zu beschränken. Informationsbroker, Werbenetzwerke, Anbieter von sozialen Netzwerken und andere Akteure in Gestalt von Unternehmen verfügen mehr denn je über vollständige Dossiers über Menschen, die an der heutigen digitalen Gesellschaft teilnehmen, und die Menschen verlieren die Kontrolle über den digitalen Fußabdruck, den sie hinterlassen. Menschen, die von Akteuren, über die sie keine Kontrolle haben oder von denen sie meist gar nichts wissen, gezielt beobachtet werden, Gegenstand einer Profilerstellung und Bewertung durch sie sind, fühlen sich hilflos und müssen in die Lage versetzt werden, Kontrolle über ihre Identität zu gewinnen. Auch wenn die Menschen formal eine Art „Hinweis“ oder die Möglichkeit erhalten haben, ihre „Einwilligung“ zu allgemeinen Geschäftsbedingungen zu geben, finden sie sich häufig in einem System wieder, das darauf angelegt ist, aus personenbezogenen Daten möglichst großen Profit zu schlagen, womit den Menschen keine echte Wahl oder Kontrolle bleibt.

2 In ihrer Mitteilung zu Big Data[1] legt die Europäische Kommission einen Aktionsplan vor, der sowohl auf den Schutz personenbezogener Daten als auch auf den Verbraucherschutz abhebt. Darin wird insbesondere dazu aufgefordert, „persönliche Datenräume“ als nutzerzentrierte, sichere und gesicherte Orte für die Speicherung personenbezogener Daten zu verwenden, an denen möglicherweise auch andere Zugriff auf diese personenbezogenen Daten erhalten können. Wir teilen die Ansicht, dass innovative digitale Instrumente und Geschäftsmodelle auf der Grundlage gestärkter Rechte natürlicher Personen gefördert werden sollten. Sie könnten natürlichen Personen gestatten, von diesem Datenaustausch zu profitieren, also an der Verwendung und Verbreitung ihrer personenbezogenen Informationen mitzuwirken.

3 In unserer Stellungnahme „Bewältigung der Herausforderungen in Verbindung mit Big Data“[2] haben wir dafür plädiert, die gesetzliche Verpflichtung einer wirksamen Einwilligung durch eine echte, praktische Kontrolle über personenbezogene Informationen zu ergänzen. So heißt es dort: *„…statt einem Verwaltungsaufwand gleichzukommen, könnte die Gewährung von Auskunftsrechten ein Merkmal der Dienstleistung für den Kunden werden“*, und weiter heißt es, dass Organisationen, die Big Data verwenden, *„auch bereit sein sollten, das durch die Verarbeitung personenbezogener Daten geschaffene Vermögen mit denjenigen zu teilen, deren Daten sie verarbeiten“*. In diesem Zusammenhang stellten wir fest: *„Mithilfe von persönlichen Datenbeständen könnten einige der Bedenken bezüglich des Verlustes der persönlichen Kontrolle über personenbezogene Daten ... ausgeräumt werden“*. In der kürzlich verabschiedeten Datenschutz-Grundverordnung (DSGV)[3] wurden die rechtlichen Anforderungen an die Einwilligung verschärft[4] und wurden die wirksamen, modernen Grundsätze des Datenschutzes durch Technik und des Datenschutzes durch datenschutzfreundliche Voreinstellungen[5] sowie das neue Recht auf Datenübertragbarkeit[6] eingeführt. Damit das neue Regelwerk für den Datenschutz den hohen Erwartungen gerecht werden kann, brauchen wir praxisnahe Instrumente, die Menschen dabei helfen, ihre Rechte auf unproblematische, benutzerfreundliche Weise wahrzunehmen.

4 In dieser Stellungnahme geht es um neue Technologien und Ökosysteme, mit denen Menschen in die Lage versetzt werden sollen, über die Erhebung und Weitergabe ihrer

personenbezogenen Daten Kontrolle auszuüben. Dieses Konzept wird von uns als „Personal Information Management-System“ („PIMS“) bezeichnet.[7] Das PIMS-Konzept eröffnet einen neuen Ansatz, dem zufolge Menschen Besitzer ihrer eigenen personenbezogenen Daten sind. Denkbar ist, dass es zu einem Paradigmenwechsel beim Management und der Verarbeitung personenbezogener Daten mit den entsprechenden sozialen und wirtschaftlichen Konsequenzen kommt. Die derzeitige Landschaft von Online-Diensten ist hingegen von einer kleinen Zahl von Dienstanbietern gekennzeichnet, die den Markt beherrschen und die personenbezogenen Daten von Nutzern als Gegenleistung für „kostenlose“ Dienste zu Geld machen. Häufig geht dies mit einem Machtungleichgewicht einher, bei dem der Kunde vor der Wahl steht „Friss oder stirb“, sowie mit einer Informationsasymmetrie zwischen Dienstanbietern und Nutzern, bei der nur wenig oder gar keine Transparenz für die Menschen darüber gegeben ist, was mit ihren personenbezogenen Daten eigentlich geschieht.

5 Der hinter dem PIMS-Konzept stehende Kerngedanke besteht darin, das derzeitige anbieterzentrierte System in ein System umzuwandeln, dass voll darauf abgestellt ist, Menschen zum Management und zur Kontrolle ihrer Online-Identität zu befähigen.[8] Grundsätzlich sollten Menschen in der Lage sein, darüber zu entscheiden, ob und mit wem, zu welchem Zweck und für welchen Zeitraum sie ihre personenbezogenen Informationen teilen möchten, und sie sollten sie im Auge behalten und gegebenenfalls entscheiden können, sie wieder zurückzunehmen. Es lohnt sich, der Frage nachzugehen, wie PIMS helfen könnten, einige der Bedenken bezüglich des Verlustes der persönlichen Kontrolle über personenbezogene Daten auszuräumen, der als eines der zentralen Anliegen bezüglich von Big Data häufig genannt wird.[9]

6 Dieser Ansatz zielt auf die Stärkung von Grundrechten in unserer digitalen Welt und gleichzeitig auf die Eröffnung neuer Chancen für Unternehmen ab, auf gegenseitigem Vertrauen beruhende innovative, auf personenbezogenen Daten fußende Dienste zu entwickeln. PIMS versprechen, eine neue technische Architektur und Organisation für das Datenmanagement zu bieten, aus denen „Vertrauensrahmen“ erwachsen sollen. Sie hoffen, für die Erfassung und Verarbeitung personenbezogener Daten im Zeitalter von Big Data alternative Geschäftsmodelle zu ermöglichen, die in stärkerem Maße dem europäischen Datenschutzrecht entsprechen.

7 In dieser Stellungnahme beschreiben wir kurz, was PIMS sind, welche Probleme sie lösen sollen und wie das geschehen soll.[10] Wir gehen der Frage nach, wie sie zu einem besseren Schutz personenbezogener Daten beitragen können und vor welchen Herausforderungen sie dabei stehen. Abschließend befassen wir uns mit künftigen Möglichkeiten, die von ihnen gebotenen Chancen sinnvoll zu nutzen.

2. MODELLE UND MERKMALE NEU ENTSTEHENDER PIMS

2.1. Architektur und Technologie

8 PIMS stecken noch in den Kinderschuhen. Bei ihrer Gestalt und den ihnen zugrunde liegenden Geschäftsmodellen bestehen große Unterschiede. Zu ihrem praktischen Nutzen und ihren Auswirkungen auf die Verarbeitung personenbezogener Daten liegen nur wenige Erfahrungen vor. In diesem Abschnitt werden einige der Modelle und Merkmale neu entstehender PIMS dargestellt.

Wo sind die Daten?

9 Eine wichtige Unterscheidung zwischen den verschiedenen Arten neu entstehender PIMS lässt sich anhand ihrer technischen Architektur treffen, also danach, ob die Daten lokal oder in einer Cloud gespeichert werden. Beim Modell der lokalen Speicherung werden personenbezogene Daten in Geräten von Nutzern gespeichert, also in Laptops, Smartphones, Tablets usw. Beim Modell der Speicherung in einer Cloud werden Daten hauptsächlich von Dienstanbietern (sozialen Netzwerken, Online-Office Suites, Anbietern von Gesundheitsdiensten usw.) sowie von spezialisierten cloudgestützten PIMS-Anbietern gespeichert.

10 Im Fall der cloudgestützten Konfiguration gibt es zwei Arten von Grundansätzen, die durchaus auch nebeneinander existieren können. Einige PIMS sind darauf angelegt, die Daten der Nutzer an einem Ort zu halten; andere schaffen eine logische Verknüpfung zwischen Nutzerdaten, die bei verschiedenen Dienstanbietern aufbewahrt werden können.

Wie werden Daten verarbeitet?

11 Entweder verlassen die Daten das PIMS gar nicht (in manchen Modellen werden sogar Algorithmen importiert und intern berechnet), oder die Daten werden auf sicherem Wege an die Dienstanbieter übermittelt, bei denen sie auch in verschlüsselter Form für die Verarbeitungsvorgänge gespeichert werden können. Daten und ihre Eigenschaften werden in einem interoperablen maschinenlesbaren Format gespeichert, so dass Interaktionen ohne menschliches Zutun möglich sind.

Wie werden Sicherheit und Datenschutz umgesetzt?

12 Sicherheit und Datenschutz gehören zu den wichtigsten Triebfedern von PIMS. Die Kryptographie spielt eine zentrale Rolle und ist notwendiger Bestandteil der Sicherheit der Daten sowie des gegenseitigen Vertrauens zwischen allen Akteuren in der Datenverarbeitungskette in die Echtheit und Integrität von Daten und Verarbeitung:

a) Verschlüsselung kann Vertraulichkeit von gespeicherten Daten und von Daten auf dem Übermittlungsweg gewährleisten;

b) kryptographische Merkmale können zur Überprüfung der Echtheit von Daten und zur Umsetzung der Datenschutzpräferenzen von Nutzern wie zugelassene Zwecke und erlaubte Speicherfristen gegenüber Dienstanbietern und Dritten verwendet werden.

13 In einigen Modellen treten Dritte (öffentliche oder private Einrichtungen) als neue Akteure in den Datenmanagement-Ökosystemen als besonders vertrauenswürdige Dienstanbieter auf. Ihre Aufgabe besteht darin, gegenseitiges Vertrauen im Wesentlichen zwischen Nutzern und Dienstanbietern herzustellen, und zwar als Identitätsanbieter und Wächter, die Authorisierungsmechanismen erleichtern und die Rückverfolgbarkeit von personenbezogenen Daten und an ihnen vorgenommenen Verarbeitungen ermöglichen.

14 Angeboten werden ferner Dienste in den Bereichen Datenminimierung und Anonymisierung. So kann beispielsweise ein Vorgang ablaufen, bei dem die Authorisierung nicht von einer vollständigen Offenlegung der Identität abhängt (so kann z. B. das PIMS, anstatt Name und Geburtsdatum abzufragen, bestätigen, dass ein Nutzer die Altersanforderungen erfüllt).[11] In anderen Fällen bieten PIMS Anonymitätsdienste[12] gegenüber Dienstanbietern und anderen die Daten verwendenden Parteien an[13], beispielsweise durch Aggregierung der Daten vor ihrer Übermittlung an diese Parteien.

2.2. Hauptmerkmale, die Personen die Kontrolle über ihre personenbezogenen Daten erleichtern

15 Eines der Hauptziele von PIMS besteht darin, Nutzern die Möglichkeit zu geben, bis zu einem bestimmten Detailgrad festzulegen, wie und für welche Zwecke ihre personenbezogenen Informationen verwendet werden dürfen, und sie in die Lage zu versetzen, mitzuverfolgen, wie diese Informationen verwendet werden, damit sie sicher sein können, dass sie nicht in einer von ihnen nicht zugelassenen Weise verwendet werden. Dies impliziert eine umfassende Funktionalität für das Einwilligungsmanagement, damit Nutzer bei Bedarf auch ihre Einwilligung zurücknehmen können. In der Regel steht für diesen Zweck eine benutzerfreundlich gestaltete Kontrollkonsole zur Verfügung. Die anderen Parteien (andere Nutzer und Dienstanbieter) können normalerweise je nach den festgelegten Datenschutzpräferenzen automatisch auf die Daten zugreifen.

16 Abgesehen von Identifizierung, Authorisierung und Management von Datenschutzpräferenzen bieten PIMS häufig weitere Mehrwertdienste. Einige PIMS bieten die Möglichkeit, Daten über die Online-Präsenz des Nutzers (wie Browserverlauf, Lesezeichen, Adressbücher, Anmeldedaten, Ortungsdaten, Finanzdaten, Aktivitäten in sozialen Netzwerken) aufzuspüren und sie im PIMS zu organisieren.

17 Eine sehr interessante Entwicklung bei PIMS ist die Möglichkeit, persönliche Analysemerkmale aufzunehmen. Dies würde das neue Paradigma unterstützen, dem zufolge Nutzer die Kontrolle über ihre Daten und darüber haben, was die Daten über sie aussagen. In einer hypothetischen Welt, in der alle einen Nutzer betreffenden Informationen diesem zur Verfügung stehen, könnte der Nutzer einen datenschutzfreundlichen persönlichen Assistenten haben, der kontrolliert, wie Informationen aus seinem persönlichen „Big Data"-Speicher verwendet werden. Dies könnte in einem sektorspezifischen Kontext (z. B. Daten betreffend Wohlergehen und Gesundheit, persönliche Mobilität) oder aus ganzheitlicher Perspektive geschehen, bei der dann über eine Person aus verschiedenen Quellen und in verschiedenen Kontexten erhobene Daten aggregiert würden. Nutzer würden kontrollieren können, wie ihre personenbezogenen Informationen und/oder daraus gewonnene Erkenntnisse im Einklang mit ihren Präferenzen und zu gegenteiligem Nutzen an externe Parteien weitergegeben werden.

2.3. Politischer Rahmen und Geschäftsmodelle für PIMS

18 Für PIMS ist mehr erforderlich als eine auf einer angemessenen Technologie beruhende neue Datenmanagement-Architektur. Darüber hinaus kommt einer gemeinsam vereinbarten Politik, dem Vertrauen in deren Umsetzung sowie Mechanismen für die Überwachung und Überprüfung dieses Vertrauens und Abhilfemaßnahmen für den Fall, dass etwas falsch läuft, ebenso große Bedeutung zu, damit in einem selbstregulierten Umfeld, das auf dem Rechtsrahmen aufbaut, tatsächlich Sicherheit und Datenschutz gewährleistet sind.

19 Daher schlagen einige Organisationen[14] PIMS vor, in denen das sichere und datenschutzfreundliche Management personenbezogener Daten durch Beiträge vieler Akteure mit verschiedenen Funktionen im Rahmen einer einzuhaltenden Strategie und einer Governance-Regelung gewährleistet wird. Grundgedanke ist, neue, auf Transparenz und Fairness beruhende Gemeinschaften des Vertrauens aufzubauen, in denen herkömmliche Online-Dienstanbieter, neue Wirtschaftsteilnehmer (z. B. Anbieter von

PIMS-Diensten und Vertrauensanbieter) und die Menschen, deren personenbezogene Daten verwaltet und verarbeitet werden, jeweils einen angemessenen Teil der Vorteile von Big Data für sich beanspruchen können.

20 Grundlage der derzeit vorherrschenden Geschäftsmodelle für PIMS-Anbieter (und andere Akteure, die das ganze Ökosystem ermöglichen) sind Online-Dienstanbieter und Dritte, die Gebühren entrichten oder Einnahmen teilen, um die PIMS-Regelung/-Dienste nutzen zu können. Generell würden die Menschen gerne kostenlose PIMS-Dienste nutzen, möglicherweise mit einigen Ausnahmen bei Extradiensten, die von PIMS-Betreibern oder deren Geschäftspartnern direkt angeboten werden.

3. WIE KÖNNEN PIMS DIE DATENSCHUTZGRUNDSÄTZE UNTERSTÜTZEN?

21 PIMS stehen vor großen Herausforderungen, denn sie möchten die Standardlösung für das Management personenbezogener Daten auf einem Markt werden, der von einer kleinen Zahl von Betreibern beherrscht wird, die häufig kein Interesse an der Schaffung von Synergien mit ihnen haben dürften.[15] Dessen ungeachtet verdienen PIMS Unterstützung und Investitionen, denn sie können viele der Datenschutzgrundsätze, Tools und Garantien unterstützen, die das Herzstück der neuen DSGV ausmachen.

22 Von wesentlicher Bedeutung ist Unterstützung derjenigen PIMS, die sich wirklich darum bemühen, Lösungen einzusetzen, die im Einklang mit der Datenschutzvision der EU und ihrem Rechtsrahmen stehen. Dies müsste einhergehen mit einer wirksamen Durchsetzung der rechtlichen Garantien für den Schutz der Nutzer vor einer unrechtmäßigen Verarbeitung ihrer Daten und vor in ihre Privatsphäre eindringenden Techniken des Nachverfolgens von Verhalten und der Profilerstellung, mit denen zentrale Grundsätze des Datenschutzes umgangen werden sollen.

23 In den folgenden Abschnitten gehen wir näher auf diese Grundsätze, Tools und Garantien ein und befassen uns mit den in diesem Zusammenhang zu bewältigenden Herausforderungen.

24 Folgende Aspekte sollten betrachtet werden: Wie werden die Datenschutzgrundsätze tatsächlich umgesetzt (z. B. Rechte der betroffenen Person, Mechanismen für eine gültige Einwilligung, Funktion des Verantwortlichen und Haftung, Datenschutz durch Technik, Sicherheit); Interoperabilität und technische Machbarkeit; Geschäftsmodelle und betroffene Interessen in PIMS; Eigentum an personenbezogenen Daten im PIMS-Kontext.

3.1. Wirksames Einwilligungsmanagment für eine echte Nutzerkontrolle und die Verwendung automatisierter Mechanismen

25 Das Einwilligungsmanagement gehört zu den Kernfunktionen von PIMS, bei dem ein automatisierter Abgleich von Nutzerpräferenzen und Anfragen nach personenbezogenen Daten vorgenommen wird. Von entscheidender Bedeutung ist, dass Datenschutzpräferenzen mit ausreichendem Detailgrad zum Ausdruck gebracht werden und einen komplexen Kontext möglicher Optionen berücksichtigen. Vor allem in Fällen, in denen das Wesen der Daten und die Art der Verarbeitung große Risiken für die betroffenen Menschen mit sich bringen könnten, sollte ihr Bewusstsein für den Kontext geschärft werden und sollten im PIMS Mechanismen für das Auslösen eines Eingreifens

durch den Menschen vorhanden sein. Es wäre auszuloten, ob es sinnvoll wäre und wenn ja, unter welchen Garantien und Bedingungen, die Einwilligung für breitere, umfassendere Kontexte wie beispielsweise Bereiche der medizinischen Forschung zu erteilen.

26 Wichtig ist auch, dass diese automatisierten Mechanismen in regelmäßigen Abständen mit dem tatsächlichen aktuellen Willen der Person durch ad hoc-Erinnerungen zur Vermeidung von Risiken abgeglichen werden, die sich aus der Unfähigkeit (oder anderen Gründen) von Personen ergeben, ihre Präferenzen zu ändern.

27 Die Verwendung von maschinenlesbaren Formen der Äußerung von Datenschutzpräferenzen, die entweder mit den Daten reisen (häufig als „sticky policies“ bezeichnet) oder logisch mit den Daten verknüpft sind, sowie von Protokollen, die ihren Austausch ermöglichen, hat noch keinen Eingang in den Markt gefunden und bedarf noch weiterer Investitionen, um sich in der Realität durchzusetzen. In der Vergangenheit stand dieses Thema im Mittelpunkt mehrerer Projekte[16], an die sich weitere Entwicklungen anschlossen[17], die durchaus Aufmerksamkeit verdienen und auf eine mögliche weitere Unterstützung geprüft werden müssen.

28 Eine gültige Einwilligung muss vor allem in informierter Weise erteilt worden sein.[18] Vertrauensrahmen, die die Nutzung von PIMS durch natürliche Personen und andere Akteure regeln (siehe Abschnitt 2.3), sehen verbindlich Transparenz und Information vor. Es sei noch darauf hingewiesen, dass ungeachtet der Forschungsbemühungen bezüglich der Verwendung maschinenlesbarer Datenschutzhinweise unter bestimmten Gegebenheiten Menschen sich bei der Prüfung der Qualität und Angemessenheit der ihnen gegebenen Informationen noch immer auf ihr Urteilsvermögen verlassen werden müssen.

3.2. Nutzer mit Kontrolle, Recht auf Auskunft und auf Berichtigung, Recht auf Datenportablität, Datenqualität

29 Der Hauptzweck von PIMS besteht darin, Nutzern Kontrolle über ihre personenbezogenen Informationen zu verschaffen. Sinnvoll gestaltete PIMS dienen nicht nur als wirksamer und benutzerfreundlicher Mechanismus für die Erteilung oder Rücknahme der Einwilligung, sondern sie erleichtern den Nutzern auch die Ausübung ihres Rechts auf Auskunft über ihre Daten und ihres Rechts, diese auf dem neuesten Stand zu halten und für ihre Richtigkeit zu sorgen, und verbessern damit die Qualität der Daten. PIMS gehören zu den meistversprechenden Anstrengungen, durch Technik das Recht auf Auskunft und Berichtigung und das neue Recht auf Datenportabilität umzusetzen.[19] Sie könnten ferner die Richtigkeit der Daten verbessern[20] und eine befristete Verwendung gewährleisten und damit zur Einhaltung des Grundsatzes der Speicherbegrenzung[21] beitragen.

30 Zwar verfolgen die meisten, wenn nicht sogar alle bestehenden PIMS diese Ziele und verfügen auch über die entsprechenden Merkmale, doch bedeutet das nicht zwangsläufig, dass es überhaupt nicht mehr zu einem eventuellen Verlust der Vertraulichkeit und zu unfairer Verwendung der Daten kommt. Mit technischen Maßnahmen lässt sich zwar aufdecken und nachweisen, was schief gelaufen ist, wenn aber Daten ein PIMS unverschlüsselt verlassen, oder wenn Daten zwar rechtmäßig beschafft, in der Folge aber von einer Organisation entschlüsselt werden, die ihre Verpflichtungen nicht einhält, besteht die Gefahr, dass Daten abgerufen und abweichend von ihrer im PIMS konfigurierten gestatteten Verwendung benutzt werden. Es ist also Vorsicht geboten und muss überprüft werden, was PIMS der Werbung nach tun und was sie in der Realität tun.

31 Die Benutzerfreundlichkeit von PIMS und die Fähigkeit der Nutzer, durch ihren Einsatz die gewünschten Wirkungen zu erzielen, ist ebenfalls äußerst wichtig, vor allem mit Blick auf das Risiko einer Exposition personenbezogener Daten einschließlich sensibler Daten gegenüber einem automatisierten Verbrauch durch Online-Dienste. PIMS-Dienste sollten durch ausführliches Schulungsmaterial und schrittweise Anleitungen und Kurse ergänzt werden, auch wenn sie eigentlich einfach anzuwenden sein sollten. Anbieter und Entwickler sollten bedenken, dass die Systeme von der breiten Öffentlichkeit genutzt werden sollen, die nicht zwangsläufig über Kompetenzen und Kenntnisse bezüglich Technik und Datenschutz verfügt.

3.3. Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen, Interoperabilität

32 Anbieter von Online-Diensten, die aufgrund des Anbietens ihrer Dienste als Verantwortliche fungieren, könnten bei der Einhaltung der Verpflichtung zum Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen dadurch unterstützt werden, dass ihre Dienste in die Lage versetzt werden, über eine Schnittstelle mit PIMS zu laufen, die den Datenschutzvorschriften der EU entsprechen, und dass ermöglicht wird, die personenbezogenen Daten der Nutzer einfach und bequem zu den einzelnen PIMS zu exportieren, Einholung und Management der Einwilligung der Nutzer, Transparenz und Rechenschaftspflicht, Sicherheit beim Datenaustausch sowie Authorisierungsmechanismen müssten sich auf die Merkmale von PIMS verlassen können. Das bedeutet, dass dem Verantwortungsgefühl von Betreibern von PIMS bei deren Konzeption in Einklang mit der DSGV grundlegende Bedeutung zukommt. Politische Entscheidungsträger sollten PIMS daher bei der Gestaltung ihrer Dienste insbesondere mit dem Ziel unterstützen, die Einhaltung der DSGV zu fördern.

33 Interoperabilität ist eine zentrale Anforderung, der sich PIMS stellen müssen[22]. Von Seiten der entstehenden PIMS-Industrie sind intensivere Normungsbemühungen erforderlich, und diese Bemühungen sollten von den politischen Entscheidungsträgern unterstützt werden.

3.4. Technische Mittel zur Einschränkung der Weiterverwendung personenbezogener Daten

34 Grundlage für die Durchsetzung von Einwilligung und Zweckspezifikation/-bindung und Datenspeicherung auf einen automatischen Abgleich individueller Präferenzen mit dem Online-Angebot (Abschnitt 3.1) sind gegenseitiges Vertrauen und eine ex post-Überprüfung der Frage, ob angemessene technische Sicherheitsvorkehrungen bestehen. Wie bereits erwähnt, sind Lösungen gefunden worden[23], die dafür sorgen, dass diese Vorschriften automatisch überprüft und durchgesetzt werden, womit ein Zugriff auf die Daten verhindert wird, sollte den Vorschriften nicht Genüge getan werden. Kryptographie unterstützt die Überprüfung der Identität des Datenverbrauchers, den Abgleich mit den erlaubten und den angegebenen Zwecken, und sie garantiert die Integrität der Daten und der für die Kontrolle verwendeten Parameter. Möchte beispielsweise ein Anbieter von Online-Diensten personenbezogene Daten, die in verschlüsselter Form ausgetauscht werden, für andere als die von der betreffenden Person erlaubten Zwecke verwenden, wird ein Zugriff dadurch verhindert, dass die entsprechenden Entschlüsselungsschlüssel nicht verfügbar sind.[24]

35 Eine erfolgreiche Kontrolle über personenbezogene Daten im Zeitalter des Internets der Dinge und von Big Data ist nur mit einer automatisierten und zuverlässigen, doch durchaus kontrollierten Durchsetzung von Datenschutzvorschriften möglich. Unserer Auffassung nach handelt es sich hierbei um einen kritischen Bereich, auf den sich Forschungsbemühungen und Investitionen konzentrieren sollten.

3.5. Transparenz und Rückverfolgbarkeit

36 Nicht bei allen Verarbeitungen personenbezogener Daten bildet Einwilligung die Rechtsgrundlage. So dürften sich beispielsweise eGovernment-Anwendungen eher auf einschlägiges EU-Recht oder nationale Rechtsvorschriften oder eine andere Rechtsgrundlage wie das Erfordernis der Wahrnehmung einer Aufgabe im öffentlichen Interesse stützen.[25] Aber selbst in diesen Fällen können PIMS kontrollieren, wie Daten zu mehr Transparenz und Rückverfolgbarkeit beitragen können. PIMS könnten es nämlich leichter machen, Bürger über Übermittlungen im Einklang mit den geltenden Datenschutzvorschriften zu informieren. Mit einem Blick auf die Kontrollkonsole in ihren PIMS könnten nämlich Bürger in Erfahrung bringen, ob ihre personenbezogenen Daten zwischen zwei Behörden in Fällen ausgetauscht wurden, in denen Übermittlungen im Gesetz geregelt sind. Auch wenn Daten für einen spezifischen Zweck auf einer anderen Rechtsgrundlage verarbeitet werden, können PIMS den betroffenen Personen dabei helfen, ihre Einwilligung in mögliche Weiterverwendungen zu anderen Zwecken wirksam zu managen. In solchen Fällen sollten Mechanismen, mit denen die Person über eine mögliche Zweckänderung informiert und davor gewarnt wird, so gestaltet werden, dass sie die Einhaltung der Datenschutzgrundsätze fördern.

3.6. Datensicherheit

37 Identifizierungs- und Authentifizierungsmechanismen in PIMS können von Forschung und Entwicklungen in anderen Zusammenhängen durchaus profitieren. Offene und skalierbare Identifizierungs-, Authentifizierungs- und Authorisierungsarchitekturen und -lösungen sind bereits im Einsatz, und es laufen Initiativen für eine Verbesserung der Technologie. Datenminimierung kann auf die Tatsache zurückgeführt werden, dass sich die Authentifizierung von der Identifizierung unterscheidet: Eine natürliche Person muss sich nicht zwangsläufig identifizieren, um die Authorisierung für den Zugang zu einer Ressource und deren Nutzung zu erhalten; vielmehr reicht es aus, eine gültige Authorisierung vorzulegen (deren „Gültigkeit“ beispielsweise gegenseitig durch einen von allen anerkannten vertrauenswürdigen Dritten gewährleistet wird).

38 Ein hohes Sicherheitsniveau ist eines der von PIMS verlangten Merkmale. Wie bereits erwähnt, machen hier die Architektur und der Einsatz von Verschlüsselung den Unterschied aus. Eine starke, sichere Verschlüsselung sollte immer wesentlicher Bestandteile von PIMS sein, damit diese halten können, was sie versprechen. Bei der Verschlüsselung kommt dem Umgang mit dem Schlüssel entscheidende Bedeutung zu. Hierzu werden verschiedene Modelle vorgeschlagen; sie reichen von der Aufbewahrung des Verschlüsselungsschlüssels lokal, also auf dem Gerät einer Person, bis zur Aufbewahrung durch den PIMS-Anbieter oder einen vertrauenswürdigen Dritten. Alle diese Modelle bergen unterschiedliche Risiken und Möglichkeiten. Auf jeden Fall kann die physische Trennung von Schlüsseln und Daten nur empfohlen werden. Die zentrale Speicherung aller oder eines erheblichen Teils der personenbezogenen Daten eines Nutzers ist allein schon riskant. Bezüglich des Speicherorts des Schlüssels sind viele

Sicherheitsexperten einmütig der Meinung, dass es riskant sein kann, Daten lokal in persönlichen Geräten zu speichern, weil diese häufig nur ein niedriges Schutzniveau aufweisen. Auf der anderen Seite bergen auch cloudgestützte Dienste ihre eigenen spezifischen Risiken. In vielen Fällen könnte es dennoch eine nachhaltige Lösung sein, die eigenen Daten einem vertrauenswürdigen PIMS anzuvertrauen, das in einem sicheren und gut gestalteten cloudbasierten Umfeld arbeitet.

39 PIMS sollten ihren Kunden gegenüber klare Aussagen zu den Vorteilen und Risiken ihrer Architektur machen, auch mit Blick auf die Art der Daten, die zu managen sie bereit sind und für die sie Rechenschaft ablegen, damit Nutzer eine Entscheidung in voller Sachkenntnis treffen können.

3.7. Übermittlungen personenbezogener Daten

40 PIMS, die nach den Grundsätzen des Datenschutzes durch Technik funktionieren, können dazu beitragen, dass Übermittlungen personenbezogener Daten über die Grenzen der Europäischen Union hinaus im Einklang mit den Vorschriften der DSGV über internationale Übermittlungen erfolgen.

41 PIMS können auch Nutzern bei der Entscheidung darüber helfen, wie weit sie geografisch betrachtet ihre Daten weitergeben wollen. Je nach den Spezifikationen der betreffenden Person können PIMS als Torwächter mit dafür sorgen, dass Daten nur insoweit reisen, als die betreffende Person dies möchte.

42 Manch einer möchte vielleicht beispielsweise nicht, dass seine Gesundheitsdaten über die Grenzen der Europäischen Union (oder vielleicht auch nur über die Grenzen des eigenen Mitgliedstaats) hinaus übermittelt werden. Andere entscheiden sich vielleicht dafür, Übermittlungen nur in Länder zu erlauben, bei denen man von einem angemessenen Schutzniveau ausgehen kann. Wieder andere sind möglicherweise bereit, die Risiken einer weiter reichenden Verbreitung von Daten einzugehen. In diesem Fall können sich PIMS die weiteren Möglichkeiten zu Nutze machen, die die DSGV für die Übermittlung personenbezogener Daten bietet. So können sie beispielsweise mit den Empfängern Vereinbarungen über Datenübermittlungen abschließen, in denen geregelt ist, dass diese Empfänger im Einklang mit dem Gesetz verbindliche vertragliche Verpflichtungen eingehen.

3.8. Funktion des Verantwortlichen und Haftung

43 PIMS könnte man als Vermittler oder „Plattformen“ bezeichnen, die als Verbindung zwischen den beiden Seiten des Marktes fungieren, nämlich einerseits natürlichen Personen, die ihre Daten zur (Wieder-)Verwendung anbieten, und andererseits Organisationen, die diese Daten (wieder-)verwenden wollen. In Anbetracht dieser besonderen Stellung ist es für PIMS wichtig, dass sie gegenüber den Personen, die ihnen ihre Daten anvertrauen, ihre Rolle und ihre Haftung klar erläutern.

44 Bezüglich einiger Aspekte der Datenverarbeitung, wie der Datenspeicherung, besteht in der Regel kein Zweifel daran, dass die PIMS als Verantwortliche handeln und daher für die Sicherung der Daten verantwortlich sind. Daher werden die PIMS allen Bestimmungen der DSGV Genüge tun müssen, beispielsweise denen über Verletzungen des Schutzes personenbezogener Daten.

45 In anderen Fällen mag die Analyse etwas schwieriger sein und wird es darauf ankommen, Rollen, Verantwortlichkeiten und Haftung klarzustellen.[26] Was geschieht z. B. bei einer

Verletzung des Schutzes personenbezogener Daten durch die Kunden der PIMS (und weniger durch die PIMS selber)? Inwieweit haftet dann das PIMS? Sind PIMS dafür verantwortlich, ihre Kunden einer Überprüfung zu unterziehen und zu gewährleisten, dass sie zuverlässig sind?

46 Ferner sollte in gleicher Weise klargestellt werden, ob die PIMS selber zur Weiterverarbeitung der Daten berechtigt sind, und wenn ja, zu welchen Zwecken und vorbehaltlich welcher Bedingungen.

47 Mit Blick auf alle Aspekte, ob es also um die eigenen Datenverarbeitungsaktivitäten der PIMS oder die ihrer Kunden geht, muss ebenfalls klargestellt werden, ob und in welchem Ausmaß PIMS ihre Haftung gegenüber natürlichen Personen, deren Daten sie besitzen, vertraglich beschränken können (es sei darauf hingewiesen, dass auf jeden Fall bezüglich der Haftung eines PIMS als Verantwortlicher, Mit-Verantwortlicher oder Auftragsverarbeiter Artikel 82 der DSGV sowieso anzuwenden ist).

3.9. Suche nach einem nachhaltigen Geschäftsmodell im Interesse der betroffenen Personen

48 Das derzeitige Erlösmodell im Internet stützt sich im Wesentlichen auf „kostenlose“ Dienste für Personen als Gegenleistung für deren personenbezogene Daten, weshalb es schwierig sein dürfte, eine ausreichende Zahl von Menschen dazu zu überreden, für ein PIMS zu zahlen. Gleichzeitig dürften Organisationen, in deren Besitz sich große Datenmengen befinden, ein ureigenes Interesse daran haben, diese Daten für sich zu behalten und zu kontrollieren (als Wettbewerbsvorteil) und Nutzern eher weniger Kontrolle einzuräumen, ob nun durch PIMS oder andere Mittel (hier könnte das in der DSGV vorgesehene neue Recht auf Datenportabilität ein gewisses Gegengewicht darstellen).

49 Für Anbieter von Online-Diensten können PIMS klare Vorteile bieten. Zum einen können PIMS die Einhaltung der DSGV erleichtern. Zum anderen können sie einen vollständigeren, gezielten und bereinigten Satz personenbezogener Daten von Verbrauchern bieten. Auf diese Weise ließen sich die Kosten für den Zugang zu solchen Daten senken.

50 Zu den denkbaren Geschäftsmodellen für PIMS, die eine gangbare Lösung für die betroffenen Personen und die PIMS selber sein könnten, gehören so genannte „freemium“-Modelle für natürliche Personen: kostenlose Basisfunktionen mit Zusatzfunktionen, z. B. individuelle Analysen zusätzlich zu den Daten gegen Zahlung. Das Anbieten von Analysen zusätzlich zu den Daten und eine teilweise Finanzierung der Plattform auf dieser Grundlage könnte an sich ein die Privatsphäre erhaltendes Konzept sein, das Analysen von Big Data zusätzlich zu personenbezogenen Informationen erleichtert.

PIMS können auch als Dienst Unternehmen oder anderen Organisationen angeboten werden, die gewillt sind, ihr Dienstangebot für ihre Kunden mit einem datenschutzfreundlichen Mittel der Interaktion zu verbessern. Erlöse entstünden in diesem Kontext durch die von den Organisationen, die die durch das PIMS gemanagten Daten verwenden, gezahlten Gebühren. Auch Einrichtungen des öffentlichen Sektors können Kunden werden, wenn sie sich mit „Personal Information Management“ befassen, um den Bürgern Gelegenheit zu geben, den Zugriff auf ihre Daten und deren Verwendung in einem „eGovernment“-Kontext zu managen, z. B. in einem Umfeld, in dem der Grundsatz „nur einmal“[27] angewandt wird.

51 Eine weitere Erwägung ist, dass einige der Wirkungen der Verwendung personenbezogener Daten (unerwünschte Werbung und ähnliches, Preisdiskriminierung bei Verkäufen über das Internet, andere Formen der Diskriminierung oder Leistungsverweigerung und ähnliches) als negative externe Effekte betrachtet werden können. Wenn dem so sein sollte, wäre es vielleicht unfair, den Nutzer für besseren Datenschutz zahlen zu lassen. Datenschutz ist ein Grundrecht und sollte nicht zu einem Privileg werden, in dessen Genuss nur der wohlhabendere Teil der Bevölkerung kommt.

52 Unabdingbar ist auf jeden Fall, die Transparenz des Geschäftsmodells gegenüber den Personen zu gewährleisten, deren Daten verarbeitet werden, damit sie wissen, um welche Interessen (von PIMS und anderen Dienstanbietern) es geht und PIMS in vollem Bewusstsein der Lage nutzen können.

3.10. Es geht mehr um die „Genehmigung der Verwendung“ personenbezogener Daten als um deren „Verkauf“

53 Das PIMS-Modell fordert eine Debatte der Frage heraus, wer eigentlich unsere personenbezogenen Daten „besitzt“. Gestützt auf Artikel 8 der EU-Charta der Grundrechte haben natürliche Personen in der EU das Grundrecht auf den Schutz ihrer personenbezogenen Daten. Die Rechte und Pflichten im Zusammenhang mit der Ausübung dieses Rechts sind in allen Einzelheiten in der vor kurzem angenommenen DSGV geregelt. Die Problematik ist nicht PIMS-spezifisch: Personenbezogene Daten werden häufig als „Währung“ für die Bezahlung so genannter „kostenloser“ Dienste im Internet wahrgenommen. Dieser Trend bedeutet jedoch nicht, dass personenbezogene Daten natürlicher Personen rechtlich als Gut betrachtet werden können, das wie jedes andere Gut auf dem Markt gehandelt werden darf. Ganz im Gegenteil: PIMS werden grundsätzlich nicht in der Lage sein, personenbezogene Daten zu verkaufen; vielmehr wird ihre Rolle darin bestehen, Dritten für konkrete Zwecke und bestimmte Zeiträume vorbehaltlich der von den natürlichen Personen selbst festgelegten Bedingungen und aller vom anzuwendenden Datenschutzrecht vorgesehenen Garantien die Verwendung personenbezogener Daten zu erlauben.

4. SCHLUSSFOLGERUNGEN UND NÄCHSTE SCHRITTE

4.1 Hin zu einer vollständigen Anwendung der DSGV

54 Wie bereits erwähnt, hat der EU-Gesetzgeber vor kurzem ein Datenschutzreformpaket verabschiedet, mit dem der Regelungsrahmen gestärkt und modernisiert wird, damit er auch im Zeitalter von Big Data greift.

55 Die neue DSGV mit Vorschriften zur Verbesserung der Transparenz und wirkungsvollen Rechten auf Auskunft und Datenübertragbarkeit sollte natürlichen Personen nicht nur mehr Kontrolle über ihre Daten verleihen, sondern auch zu effizienteren Märkten für personenbezogene Daten beitragen, zugunsten sowohl von Verbrauchern als auch von Unternehmen.

56 Verhaltenskodizes und Zertifizierungsregelungen, wie sie in der DSGV vorgesehen sind, sind bevorzugte Instrumente, mit denen Technologien und Produkten besondere Sichtbarkeit und Funktion verliehen werden kann, die - wie PIMS - dazu dienen können, das Datenschutzrecht in der Praxis wirksamer umzusetzen.

57 PIMS stehen jedoch vor der großen Schwierigkeit, dass sie sich auf einem Markt durchsetzen müssen, der von Online-Diensten beherrscht wird, die sich auf Geschäftsmodelle und technische Architekturen stützen, bei denen Menschen keine Kontrolle über ihre Daten haben, wie in Abschnitt 3.9 ausgeführt. Der Umstieg auf eine Situation, in der natürliche Personen tatsächlich die Möglichkeit haben, einem Dienstanbieter Zugriff auf einige ihrer Daten in einem PIMS zu gewähren und ihm nicht direkt die Daten einzureichen, wird zusätzliche Anreize für die Dienstanbieter erfordern. Die Kommission könnte die von ihr angekündigten Initiativen zu Datenflüssen und Eigentumsrechten an Daten[28] zur Klärung der Frage heranziehen, welche weiteren politischen Initiativen Verantwortliche motivieren könnten, diese Art der Datenbereitstellung zu akzeptieren. Ferner könnte eine Initiative öffentlicher eGovernment-Dienste, PIMS als Datenquelle an Stelle einer direkten Datenerhebung zu akzeptieren, die kritische Masse für eine Akzeptanz von PIMS vergrößern.

58 Diese Analyse könnte mit Maßnahmen ergänzt werden, mit denen das technische, gesellschaftliche und wirtschaftliche Fundament gelegt wird, einschließlich Normungsbemühungen, wirtschaftlicher Anreize und Förderung von Forschung und Pilotprojekten.

59 Die Verwaltungen der Europäischen Union und der Mitgliedstaaten und von ihnen gemeinsam finanzierte Projekte sind die ersten Stellen, an denen dieser Perspektivenwechsel getestet, gefördert und hoffentlich realisiert werden sollte.

4.2 Unterstützung von PIMS und der ihnen zugrunde liegenden Technologie für wirksamen Datenschutz

60 Gute Vorschriften sind zwar unerlässlich, reichen allein aber nicht aus. Wie wir bereits in unserer Stellungnahme „Bewältigung der Herausforderungen in Verbindung mit Big Data“[29] ausgeführt haben, sollten Unternehmen und andere Organisationen, die viel Zeit und Mühe in innovative Möglichkeiten für die Nutzung personenbezogener Daten investieren, bei der Umsetzung von Datenschutzgrundsätzen das gleiche innovative Denken an den Tag legen.

61 Die Technologie leistet einen grundlegenden Beitrag zum PIMS-Modell. PIMS können dazu dienen, Konzepte des Datenschutzes durch Technik und die sie tragenden Technologien zu testen. Nachstehend einige relevante Forschungsthemen, für die Unterstützung und Investitionen benötigt werden: interoperables und datenschutzfreundliches Identitätsmanagement; Authorisierungsmechanismen; Dateninteroperabilität; Datensicherheit; Mechanismen für die automatische Durchsetzung von „Verträgen“ zwischen natürlichen Personen und anderen Parteien. All dies erfährt seinen Durchbruch durch Kryptographie und Verschlüsselung und wird durch die billige Verfügbarkeit von Rechenleistung angeregt. Damit die derzeit bestehenden Chancen nicht ungenutzt verstreichen, ist in dieser Anfangsphase in entscheidendem Umfang Unterstützung durch politische Entscheidungsträger wie die Kommission für die Grundlagenforschung und die angewandte Forschung in diesen Technologiebereichen erforderlich.

62 Zur Förderung von Forschung und Entwicklung im Bereich der PIMS und ihres Einsatzes auf dem Markt empfehlen wir der Kommission, nach möglichen Synergien mit anderen Bereichen der Strategie für den digitalen Binnenmarkt wie Cloud Computing und Internet der Dinge zu suchen. Auf diese Weise könnten Pilotprojekte zur Gestaltung und zum

Testen der Interaktion von Cloud-Diensten und dem Internet der Dinge mit PIMS durchgeführt werden.

4.3 Wie bringt der EDSB diese Debatte voran?

63 Ziel des EDSB ist es, private und öffentliche Anstrengungen, die in die vorstehend aufgezeigte Richtung gehen, mit zu unterstützen. Wir werden auch weiterhin die Debatte fördern, auch durch Veranstaltungen/Workshops, auf denen es beispielsweise darum gehen könnte, gute Vorgehensweisen zu ermitteln, zu ermutigen und zu fördern, um größere Transparenz und Nutzerkontrolle herzustellen und die von PIMS gebotenen Möglichkeiten zu erkunden. Wir werden ferner auch in Zukunft die Arbeit des Internet Privacy Engineering Network (IPEN) als eines interdisziplinären Wissenszentrums für Ingenieure und Datenschutzexperten fördern. In diesem Zusammenhang werden wir weiterhin eine Plattform für Entwickler und Träger von PIMS bereitstellen, auf der sie sich mit Spezialisten für andere Technologien und Datenschutz austauschen können.

Marrakesch, den 20. Oktober 2016

(**gezeichnet)**

Giovanni Buttarelli
Europäischer Datenschutzbeauftragter

Endnoten

[1] Mitteilung COM(2014) 442 Für eine florierende datengesteuerte Wirtschaft: https://ec.europa.eu/digital-single-market/en/news/communication-data-driven-economy.
[2] Stellungnahme 7/2015 des EDSB: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_DE.pdf . Siehe insbesondere Abschnitt 3.
[3] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Amtsblatt der Europäischen Union L 119 vom 4.5.2016, S. 1, abrufbar unter: http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L:2016:119:FULL
[4] Siehe unter anderem Artikel 6 Absatz 1 Buchstabe a, Artikel 7, Artikel 8 und Erwägungsgründe 42f. DSGV.
[5] Artikel 25 DSGV.
[6] Artikel 20 DSGV.
[7] „Persönliche Datenbestände", „persönliche Datenräume" und „persönliche Datendepots" sind verwandte Konzepte. In dieser Stellungnahme verwenden wir den Begriff „PIMS", da er nach unserer Ansicht das Konzept allgemein und leicht verständlich beschreibt. Die in dieser Stellungnahme verwendete Abkürzung „PIMS" kann entweder als Singular oder als Plural verstanden werden, also als Personal Information Management-System oder als Personal Information Management-Systeme.
[8] Siehe Erwägungsgrund 7 der DSGV: „Natürliche Personen sollten die Kontrolle über ihre eigenen Daten besitzen". Siehe ferner beispielsweise Doc Searls, *The Intention Economy: When Customers Take Charge* (Boston: Harvard Business Review Press, 2012).
[9] Siehe zum Beispiel Ira S. Rubinstein, Big Data: The End of Privacy or a New Beginning? International Data Privacy Law, 2013, Vol 3, No 2.
[10] Siehe beispielsweise den Bericht über Persönliche Datenbestände, den die University of Cambridge für die Europäische Kommission abgefasst hat: https://ec.europa.eu/digital-single-market/en/news/study-personal-data-stores-conducted-cambridge-university-judge-business-school.
[11] Siehe unter anderem: Kai Rannenberg, Jan Camenisch, Ahmad Sabouri (eds.), *Attribute-based credentials for trust*, (Cham: Springer International Publishing, 2015).
[12] Zu näheren Einzelheiten zum Konzept der Anonymisierung und seiner Wirksamkeit siehe ferner die Stellungnahme 5/2014 der Artikel 29-Datenschutzgruppe zu Anonymisierungstechniken: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf.
[13] Siehe beispielsweise das openPDS-Projekt: http://openpds.media.mit.edu/.
[14] Siehe beispielsweise die Qiy Foundation (https://www.qiyfoundation.org/) und das Respect Network (https://www.respectnetwork.com/ und http://oixnet.org/registry/respect-network/).
[15] Siehe die vorläufige Stellungnahme des EDSB zu „Privatsphäre und Wettbewerbsfähigkeit im Zeitalter von Big Data". https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_DE.pdf. Siehe insbesondere Abschnitt 4.2.2: *„Mächtige oder marktbeherrschende Unternehmen sind in der Lage, „Aggregationsvorteile" (economies of aggregation) zu erzielen und Marktzutrittsbarrieren zu schaffen durch ihre Kontrolle enormer Mengen personenbezogener Daten sowie eigener Software, die diese Daten organisiert".*
[16] Ein sehr bekannter Versuch war das Projekt P3P W3C und die entsprechende Sprache für den Austausch von Präferenzen, APPEL.
[17] Siehe beispielsweise die Initiative Kantara (https://kantarainitiative.org/), unter deren Schirm viele Projekte durchgeführt werden, die sich für einen „sicheren Zugang zu vertrauenswürdigen Online-Diensten unter Wahrung der Privatsphäre" einsetzen.
[18] Artikel 4 Absatz 11 DSGV.
[19] Siehe Artikel 20 DSGV.
[20] Artikel 5 Absatz 1 Buchstabe d DSGV.
[21] Artikel 5 Absatz 1 Buchstabe e DSGV.

[22] Ein bemerkenswertes Beispiel ist die Verwendung der XDI Protocol Suite, vorgeschlagen von der XDI Public Trust Organisation (http://xdi.org/), die einen zuverlässigen und sicheren Datenaustausch auf der Grundlage festgelegter Kriterien (z. B. Datenschutzpräferenzen) erlaubt.

[23] Beispiele für diese Lösungen sind so genannte „smart contracts“, mit denen automatisierte Vertragsdurchsetzung und -aushandlung erreicht werden sollen. Das Konzept geht zurück auf die 1990er Jahre und den Kryptographen Nick Szabo, der es damals entwickelte (http://szabo.best.vwh.net/smart_contracts_idea.html). Aufgrund neuer Entwicklungen in der Kryptographie hat dieses Konzept in jüngerer Zeit neue Forschungsaktivitäten angestoßen.

[24] Dies geschieht in der Regel auch dank der Einbeziehung von Identitäts-/Authentifizierungsanbietern, denen alle beteiligten Parteien vertrauen, und die die Authentizität der Daten-„Attribute“ (Datenschutzpräferenzen oder andere Angaben) und der von Online-Diensten angegebenen Zwecke/Datenverwendungen sowie die Identität dieser Dienste garantieren. Ferner kann etwas bei bestimmten Ereignissen wie erfolgreicher oder erfolgloser Entschlüsselung unternommen werden, beispielsweise Meldung des Ereignisses an das PIMS, was wiederum eine Kontrolle ermöglicht.

[25] Artikel 6 Absatz 1 Buchstabe c und e DSGV.

[26] Siehe auch Artikel 82 DSGV.

[27] So wird der Grundsatz bezeichnet, dem zufolge der Staat von den Bürgern nur einmal die Vorlage von Informationen oder Dokumenten in einem Umfeld verlangen sollte, in dem Behörden gehalten sind, die Informationen oder Dokumente auszutauschen. Es könnte wünschenswert sein, diese Informationen in einer PIMS-Plattform zu speichern, damit größere Transparenz gegeben ist und die Menschen ihre Daten besser kontrollieren können.

[28] Mitteilung: Digitalisierung der europäischen Industrie - Die Chancen des digitalen Binnenmarkts in vollem Umfang nutzen http://europa.eu/rapid/press-release_MEMO-16-1409_de.htm.

[29] Bereits zitierte Stellungnahme 7/2015 des EDSB.