ORCID aus datenschutzrechtlicher Sicht

"Gutachten im Auftrag des von der Deutschen Forschungsgemeinschaft (DFG) geförderten Projektes ORCID DE zur Förderung der Open Researcher and Contributor ID in Deutschland"

RA Jan Schallaböck,
RA Max von Grafenstein LL.M.
iRights.Law Rechtsanwälte

Berlin im Mai 2017

Dieses Gutachten ist online verfügbar via http://doi.org/10.2312/lis.17.02

iRights.Law Rechtsanwälte - Klimpel, Kreutzer, Schallaböck und Weitzmann Partnerschaft
Gesellschafter: Paul Klimpel, Till Kreutzer, Jan Schallaböck, Maximilian von Grafenstein
Almstadtstraße 9/11 | 10119 Berlin | T +49.30.5459.8130 | F +49.30.7563.8797 | assistenz@irights-law.de | www.irights-law.de
Amtsgericht Charlottenburg | Registernummer PR 987 B | Finanzamt Mitte/Tiergarten | Steuer-Nr 34/398/00670 | USt-ID DE286578109
Deutsche Bank | Konto 0636399 | BLZ 20070024 | IBAN DE62 200 700 240 063 639 900 | BIC/SWIFT DEUTDEDBHAM

Inhaltsverzeichnis

Einleitung

Die eindeutige Identifikation von Forscherinnen und Forscher ist für die Wissenschaft in vielerlei Hinsicht bedeutsam. In einem System, das stark auf Reputation aufbaut, können falsche Zuordnungen von Veröffentlichungen, etwa weil ein Name nicht eindeutig ist, oder fehlende Zuordnungen, weil ein Namenswechsel stattfand, zu Verzerrungen bzw. Verwechslungen führen.

Die *Open Researcher and Contributer ID*[1] (im Folgenden „ORCID iD“) ist eine Autorenkennung durch die Wissenschaftlerinnen und Wissenschaftler global eindeutig identifiziert und ihnen Werke eindeutig zugeordnet werden können. Neben der ORCID iD wird unter www.orcid.org eine Plattform (im Folgenden „ORCID“) zur Verwaltung der Werke und weitere Angaben betrieben. Bei den meisten auf der Plattform eingestellten und verwalteten Daten handelt es sich um bereits veröffentlichte Daten (zum Beispiel Titel, Autor bzw. Autorin, Veröffentlichungsdatum und -ort eines bereits veröffentlichten wissenschaftlichen Werks). Betrieben wird ORCID von der ORCID Inc. einer Non-Profit-Gesellschaft mit Sitz in Delaware, USA.[2]

Primär adressiert das Angebot die Wissenschaftlerinnen und Wissenschaftler, indem es neben der ORCID iD ein Webportal zur Verfügung stellt, auf dem diese Informationen über ihre wissenschaftliche Tätigkeit verwalten können. Zentraler Bestandteil des Systems sind dabei die Datenschutzfunktionalitäten, die die Wissenschaftlerinnen und Wissenschaftler als Nutzende des Portals befähigen, festzulegen, wem sie welche Informationen zugänglich machen. Neben den Wissenschaftlerinnen und Wissenschaftlern selbst richtet sich ORCID an Hochschulen und außeruniversitäre Forschungseinrichtungen, darüber hinaus auch an Fachverlage sowie an andere Forscherinnen und Forscher, die den im Rahmen von ORCID erhobenen Datenbestand analysieren oder anderweitig verwenden möchten. Schließlich können die Nutzerinnen und Nutzer die Pflege des Datenbestandes an andere von ihnen benannte und vertrauenswürdige Entitäten etwa an bestimmte Einzelpersonen (zum Beispiel Mitarbeiter) delegieren. Die Entscheidung darüber, was sie über ORCID veröffentlichen, verbleibt dabei stets bei den ursprünglichen Wissenschaftlerinnen und Wissenschaftlern.

---

1 Auf Deutsch etwa „Offener Wissenschaftler- und Mitwirkenden-Identifikator“

2 ORCID Inc., Certificate of incorporation, https://orcid.org/sites/default/files/orcidincde-certificateofincorporation-121130175812-phpapp01.pdf (7.5.2017).

Zentrales technisches Element des Systems ist eine sechzehnstellige, nichtsprechende Identifikationsnummer[3], die „ORCID iD". Wissenschaftlerinnen und Wissenschaftler können für sich eine solche Identifikationsnummer auf der Webseite orcid.org erzeugen. Die Publikationen der jeweiligen Person werden mit dieser Identifikationsnummer verknüpft. Dadurch sollen Namensverwechslungen ausgeschlossen werden.[4]

ORCID stellt damit unter anderem ein nutzerzentriertes („user controlled") Identitätsmanagementsystem dar (auch als Typ 3 „Identity Management System" bezeichnet).[5] Es geht über die Funktionalität einfacher Identifikationsmanagementsysteme (auch: „Accountmanagement", Typ 1) hinaus und bietet Funktionalitäten des „Profilmanagements" (Typ 2), wobei diese Funktionalitäten in der Hand der jeweiligen Nutzerinnen und Nutzer liegen.[6] Es basiert auf einem zentralisierten Modell mit einzelnen übertragbaren Elementen, etwa in Hinblick auf die vorgenannten Delegationsmöglichkeiten sowie auf weitere Single-Sign-on-Funktionalitäten. Als Single-Sign-on werden solche Funktionen bezeichnet, bei denen ein Identitätsmanagementsystem (zum Beispiel die ORCID iD) zur Authentifizierung auch für andere Dienste eingesetzt werden kann. In jüngerer Zeit wieder vermehrt diskutierte (zumeist allerdings noch experimentelle) dezentralisierte oder distribuierte Ansätze werden von ORCID noch nicht verfolgt.[7]

Die Verarbeitung der Daten wird durch die Firma ORCID Inc. vorgenommen. ORCID Inc. betreibt ihre technische Infrastruktur zum Zeitpunkt der Erstellung dieses Gutachtens auf Servern des Anbieters Rackspace.[8] Rackspace betreibt

---

[3] „Nichtsprechend" sind Identifikationsnummern immer dann, wenn die Nummer selber keine Angaben über die betreffende Person enthält. Bei einigen Identifikationssystemen wurde etwa das Geburtsdatum als Element in die Nummer eingefügt. Von dieser Praxis machen moderne Identifikationssysteme keinen Gebrauch mehr. Das Vorliegende folgt dabei ISO 27729:2012 Information and documentation — International standard name identifier (ISNI), vgl.: http://www.iso.org/iso/catalogue_detail?csnumber=44292, und vergibt Identifikationsnummern zufällig, https://support.orcid.org/knowledgebase/articles/116780-structure-of-the-orcid-identifier (7.5.2017).

[4] Vgl. http://orcid.org.

[5] Dargestellt etwa hier: Jøsang, Audun; Rosenberger, Christophe; Miralabé, Laurent; Klevjer, Henning; A Varmedal, Kent; Daveau, Jérôme; Husa, Knut Eilif; Taugbøl, Petter: „Local user-centric identity management" (2015), in: Journal of Trust Management 2:1 DOI 10.1186/s40493-014-0009-6, online: doi: http://doi.org/10.1186/s40493-014-0009-6.

[6] Klassifikation nach Bauer, Matthias; Meints, Martin; Hansen, Marit: „FIDIS Deliverable 3.1: Structured Overview on Prototypes and Concepts of Identity Management Systems" (2005), online: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.1.overview_on_IMS.final.pdf (17.3.2017).

[7] Vgl. Quentin Hardi in der New York Times vom 7. Juni 2016: „The Web's Creator Looks to Reinvent It", online: https://www.nytimes.com/2016/06/08/technology/the-webs-creator-looks-to-reinvent-it.html. Zu den Begrifflichkeiten schon: Baran, Paul. "On distributed communications networks." *IEEE transactions on Communications Systems* 12.1 (1964): 1-9 (2). Online: https://www.rand.org/content/dam/rand/pubs/research_memoranda/2006/RM3420.pdf.

[8] Wir schließen dies aus der Tatsache, dass die für www.orcid.org registrierte IP-Adresse zum Adressraum des Anbieters Rackspace gehört.

neben Servern in den USA auch Server in London, Hong Kong und Sydney.[9] Das impliziert, dass die Daten auch auf Server in den USA transferiert, dort gespeichert und von dort von den genannten Stakeholdern abgerufen werden können. ORCID Inc. behält sich das Recht zur Verarbeitung an anderen Orten als dem Aufenthaltsort des Nutzers in Nr. 12 der Datenschutzerklärung[10] ausdrücklich vor.

Der Sourcecode der technischen Plattform liegt unter einer MIT-Lizenz vor und ist für jeden offen einsehbar.[11] Ebenso verfügbar sind die technischen (Programmier-)Schnittstellen (englisch: „Application Programming Interfaces", kurz: APIs), die es der Öffentlichkeit teilweise und den Mitgliedern umfassender ermöglichen, die bei ORCID hinterlegten Informationen semantisiert und automatisiert abzurufen und im Falle der Mitglieder auch Daten auf diesem Wege einzuspeisen.[12]

ORCID erfreut sich seit dem Start im Jahr 2012 eines erheblichen Zulaufs, auch in Deutschland. Daher hat sich das von der Deutschen Forschungsgemeinschaft (DFG) geförderte Projekt „ORCID DE" entschlossen, dieses Gutachten zu beauftragen, mit der zentrale datenschutzrechtliche Aspekte beleuchtet werden sollen.[13]

Der Schwerpunkt des Gutachtens soll darauf liegen, wie ORCID an wissenschaftlichen Einrichtungen in Deutschland implementiert wird. Dabei werden die institutionellen Regularien sowie die deutschen und europäischen Normen, denen wissenschaftliche Einrichtungen in Deutschland unterliegen, die ORCID implementieren, betrachtet. Dabei soll auch der Tatsache Rechnung getragen werden, dass dabei Datenflüsse in die USA entstehen. Zentrale Anforderung ist, dass das Gutachten möglichst allgemein verständlich und allgemeingültig formuliert wird und somit einen Orientierungsrahmen für die rechtliche Prüfung vor Ort, also etwa an Hochschulen und außeruniversitäre Forschungseinrichtungen bietet. Anliegen des Gutachtens ist es, wissenschaftliche Einrichtungen bei der rechtskonformen Umsetzung der Autorenidentifikation mit ORCID zu unterstützen.

---

[9] Rackspace Inc. „Global Infrastructure", online: https://www.rackspace.com/about/datacenters (31.3.2017). Ein Serverstandort in Frankfurt ist angekündigt und soll Mitte 2017 verfügbar sein; vgl. Yahoo Finance, „Rackspace opens first data center in continental Europe", online: https://finance.yahoo.com/news/rackspace-opens-first-data-centre-140000321.html (21.3.2017).

[10] ORCID, „Privacy Policy", online: https://orcid.org/privacy-policy (17.3.2017).

[11] Unter https://github.com/ORCID/ORCID-Source.

[12] Übersicht: https://orcid.org/organizations/integrators/API.

[13] Bertelmann, R., Niggemann, E., Pieper, D., Elger, K., Fenner, M., Hartmann, S., Höhnow, T., Jahn, N., Müller, U., Pampel, H., Schirrwagen, J., Summann, F. (2015): „ORCID DE – Förderung der Open Researcher and Contributor ID in Deutschland". doi: http://doi.org/10.2312/lis.16.01.

Der Erstellung des Gutachtens ging ein Prozess voraus, der die Zusammenarbeit mit dem DFG-Projekt ORCID DE gewährleisten sollte. So wurden im November 2016 im Rahmen eines Workshops nach Darstellung grundsätzlicher Datenschutzprinzipien spezifische Fragestellungen erarbeitet (Annex I[14]); im Rahmen eines weiteren „Community Inputs" (Annex II[15]), der über das Projekt ORCID DE gesammelt wurde, wurden weitere Aspekte adressiert.

Eingeflossen in das Gutachten ist ebenfalls eine Korrespondenz mit den Betreibern von ORCID, in der zu einzelnen Fragen, die im Rahmen der Bearbeitung aufgetaucht sind, Stellung genommen wurde.

[14] Annex I und Annex II sind in der öffentlich zugänglichen Fassung dieses Gutachtens aus Gründen des Datenschutz- und des Urheberrechts nicht enthalten.
[15] S.o.

I. Methode und Gang der Untersuchung

Der Methodenkoffer der Datenschutzberatung enthält eine Vielzahl von Herangehensweisen. Neben den typischen gesetzlichen Aufgaben der Prüfung von Verfahrensverzeichnissen, der Durchführung von Vorabkontrollen (zukünftig: Datenschutzfolgeabschätzungen oder „Data Protection Impact Assessments"), der Entwicklung von Datenschutzkonzepten oder einem Datenschutzmanagementsystem, zählt hierzu die verfassungsverträgliche und die datenschutzfreundliche Technikgestaltung („Privacy by Design"). Daneben und übergreifend steht die rechtliche Begutachtung von Anwendungsszenarien, konkreten Fällen und die Beurteilung von Erfolgsaussichten für Rechtsstreitigkeiten, die der klassischen rechtlichen Methodenlehre folgen. Schließlich berührt der Datenschutz regelmäßig Fragen der Prozessorganisation, ethische Fragestellungen und solche, die aufgrund der Dynamik der jüngeren Entwicklungen (noch) nicht Eingang in das Recht gefunden haben. Da in aller Regel eine Vielzahl von Interessen und Grundrechten zu berücksichtigen sind, spielen bei nahezu allen Methoden (Risiko-)Abwägungen eine wichtige Rolle.

Zur Bearbeitung der aufgeworfenen datenschutzrechtlichen Fragestellungen erschien eine Strukturierung entlang von Anwendungs- oder Nutzungsszenarien sinnvoll. Diese Herangehensweise eignet sich als Abstraktion der rechtlichen Begutachtung für die vorliegenden Fragestellungen besonders gut. Da das technische System von ORCID bereits weitgehend definiert ist, sind rückwirkend technikgestaltende Ansätze weitgehend nicht im Zentrum der Betrachtung. Allerdings sieht das System von ORCID ohnehin einige wesentliche Mechanismen vor, die dem Nutzer oder der Nutzerin eine weitgehende Kontrolle der Datenverwaltung ermöglichen. Dementsprechend kann die abstrahierte rechtliche Beurteilung Hinweise darauf liefern, inwieweit das bestehende System den rechtlichen Anforderungen entspricht. In diesem Sinne kann die rechtliche Analyse insbesondere aufdecken, ob in der Gestaltung die richtigen Risikoabwägungen vorgenommen wurden. Schließlich ist die fallorientierte Herangehensweise auch deswegen sinnvoll, weil sie im Datenschutzrecht in dem Prinzip der Zweckbindung ein ähnlich strukturiertes Element findet. Daneben werden technische Systeme oft entlang von sogenannten „Use Cases" entwickelt, was wiederum den hier zugrunde liegenden Anwendungsszenarien im weitesten Sinne entspricht. Stellenweise werden aber auch Bezüge zu anderen Methoden hergestellt.[16]

[16] Wir weisen darauf hin, dass dieses Gutachten keine vollständige rechtliche Prüfung aller konkreten Nutzungen von ORCID abbilden kann. Ebenso wenig kann es eine „datenschutzrechtliche Unbedenklichkeitsbescheinigung" liefern. Dies muss – sofern überhaupt möglich - anderen Verfahren vorbehalten bleiben. Zu denken ist hier etwa an das Datenschutzgütesiegel EuroPrise. Dieses bietet eine Methodologie, die in diese Richtung geht; allerdings erlaubt auch dieses Gütesiegel lediglich die Aussage, dass sich eine Technologie grundsätzlich rechtskonform einsetzen lässt. Alternativ oder zusätzlich ist an eine Vorabkontrolle zu denken, die bei Datenverarbeitungen mit

Nach einer groben Umschreibung der Funktionalitäten von ORCID im Rahmen des Untersuchungsgegenstandes (II.) sollen zunächst allgemeine datenschutzrechtliche Fragen geklärt werden (III.), um schließlich spezifische Rechtsfragen genauer zu betrachten (IV.). Im Fazit (V.) finden sich schließlich auch Empfehlungen, die sich für die Fortentwicklung der Plattform ergeben können.

hohem Risiko für Betroffene gesetzlich vorgeschrieben ist. Zunehmend wird sie von Organisationen auch routinehalber durchgeführt, auch wenn – wie wohl auch im Falle von ORCID – das Risiko nicht als hoch zu qualifizieren ist. Dieses Gutachten kann für in diesem Rahmen ergänzend herangezogen werden, es kann aber – in Ermangelung des Wissens um die konkreten Abläufe und einen Einblick in die konkrete technische Implementierung in bzw. bei ORCID – eine Vorabkontrolle nicht gänzlich ersetzen.

II. Untersuchungsgegenstand

In diesem Abschnitt soll eine Darstellung typischer Anwendungsszenarien von ORCID erfolgen. Für die darauffolgende rechtliche Betrachtung in den Abschnitten III. und IV. haben sich die Verfasser entschieden, eine Reihe verschiedener Fallgruppen entlang rechtlicher Kategorien herauszugreifen. Demgegenüber folgt die hiesige Darstellung noch der Perspektive der Wissenschaftlerinnen und Wissenschaftler (im Folgenden auch „die Nutzerinnen und Nutzer" und – sofern die datenschutzrechtliche Betroffenheit thematisiert wird – „die Betroffenen"), die das Portal nutzen.

Damit beginnt die Darstellung in diesem Abschnitt mit dem Anlegen eines Profils (1.), erläutert dann das Erstellen und Bearbeiten der Informationen (2.) und schließlich die Nutzung der Daten auch durch Dritte (3.).[17] Umrissen werden auch weitere Funktionen, insbesondere im Bereich des Identitätsmanagements (4.) gefolgt von einer kurzen Zusammenfassung (5.).

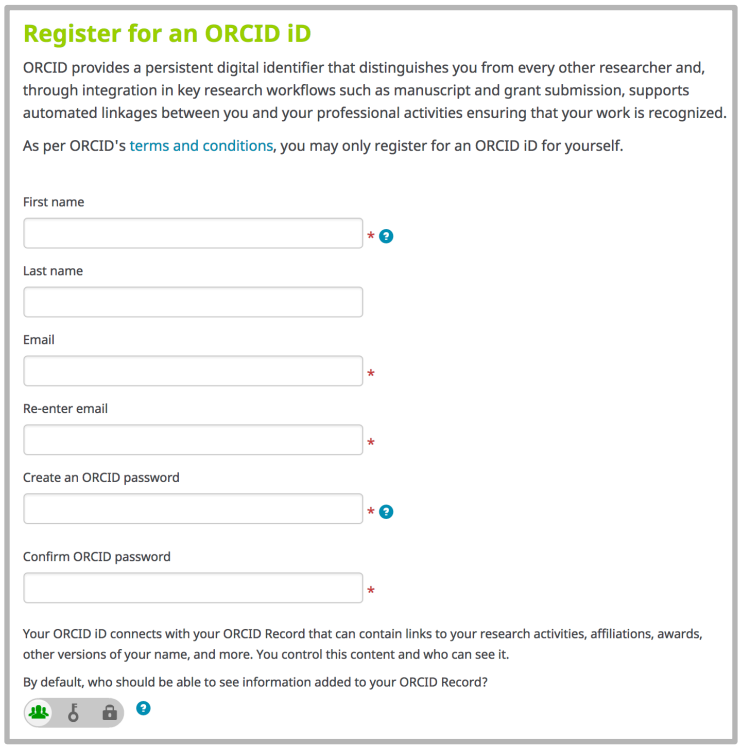

Abbildung 1: Registrierung

1. Anlegen eines ORCID-Profils

Nutzerinnen und Nutzer können auf dem ORCID-Portal zunächst ihr persönliches Profil anlegen. Hierfür müssen sie einen Vornamen, ihre E-Mail-Adresse und ein Passwort hinterlegen (siehe Abbildung 1).

a) Privacy-Funktionalität: Voreinstellungen

Im Rahmen dieses Registrierungsprozesses können sie außerdem die allgemeinen Privacy-Voreinstellungen anpassen. Sie können dabei auswählen, ob die Informationen in ihrem Profil grundsätzlich öffentlich (im Folgenden auch

[17] Auf die unterschiedlichen Definitionen und Abgrenzungen zwischen den Begriffen „Datum" und „Information" wird im Folgenden nicht näher eingegangen, da sie für die hier untersuchten Fragestellungen nicht relevant werden. Aus rechtlicher Sicht können sie in diesem Zusammenhang weitgehend als synonyme Begriffe verstanden werden, obgleich das gängige Verständnis von Daten als digitale Repräsentation von Information gelegentlich auch in der Rechtswissenschaft herangezogen wird. Dabei spielt regelmäßig auch der Gedanke eine Rolle, dass wiederum die Gewinnung von Information aus Daten ein Zusatzwissen erfordert, das über die bloße Repräsentation der ursprünglichen Information hinausgeht.

„public“), grundsätzlich vertraulich (im Folgenden auch „private“) oder grundsätzlich nur bestimmten vertrauenswürdigen Personen (im Folgenden auch „limited access“) zugänglich gemacht werden.[18]

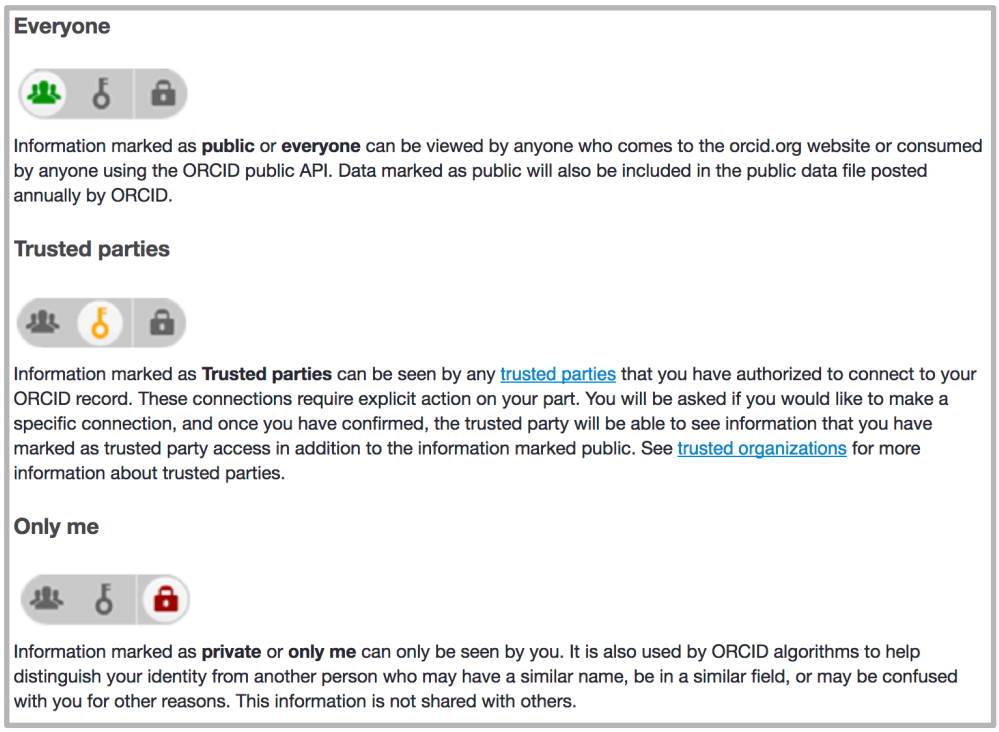

Abbildung 2: Datenschutz-Einstellungen

Die Abbildung 2 zeigt die Privacy-Funktion, über die die Nutzerin oder der Nutzer die Privacy-Voreinstellung mithilfe des Schalters einer der drei Kategorien zuordnen kann.[19] Die Privacy-Voreinstellung steht von Werk aus („by default“) auf „public“. Die Nutzerin oder der Nutzer kann diese Privacy-Voreinstellung im Rahmen der Registrierung sowie zu jedem Zeitpunkt grundsätzlich auf „private“ oder „limited access“ umstellen. Letzteres bedeutet, dass die Angabe nur bestimmten vertrauenswürdigen Personen (im Folgenden „trusted parties“) zugänglich sein soll.[20] Diese Privacy-Funktion wird hier Voreinstellung genannt, weil sie für *alle* eingepflegten Profilangaben gilt. Zusätzlich kann die Nutzerin oder der Nutzer aber auch jede *einzelne* Angabe spezifisch auf „private“, „public“ oder „limited access“ stellen.[21]

---

[18] Siehe unter https://orcid.org/register.

[19] Siehe Punkt 4.1 der Privacy Policy von ORCID unter https://orcid.org/content/orcid-privacy-policy#TrustedIndividual (im Folgenden auch „Privacy Policy“) sowie unter http://support.orcid.org/knowledgebase/articles/124518-orcid-visibility-settings (23.3.2017).

[20] Siehe sogleich im Detail unter Abschnitt 2.

[21] Siehe hierzu sogleich unter Punkt II. 2. b) „Privacy-Funktionalität: Spezifische Einstellungen“.

b) Einwilligungserklärung

Zum Abschluss der Registrierung muss die Nutzerin oder der Nutzer durch aktives Anklicken eines vom sonstigen Text grafisch abgesetzten Kästchens seine oder ihre Einwilligung zu der verlinkten Datenschutzerklärung (im Folgenden auch „Privacy Policy“) abgeben (siehe Abbildung 3).[22]

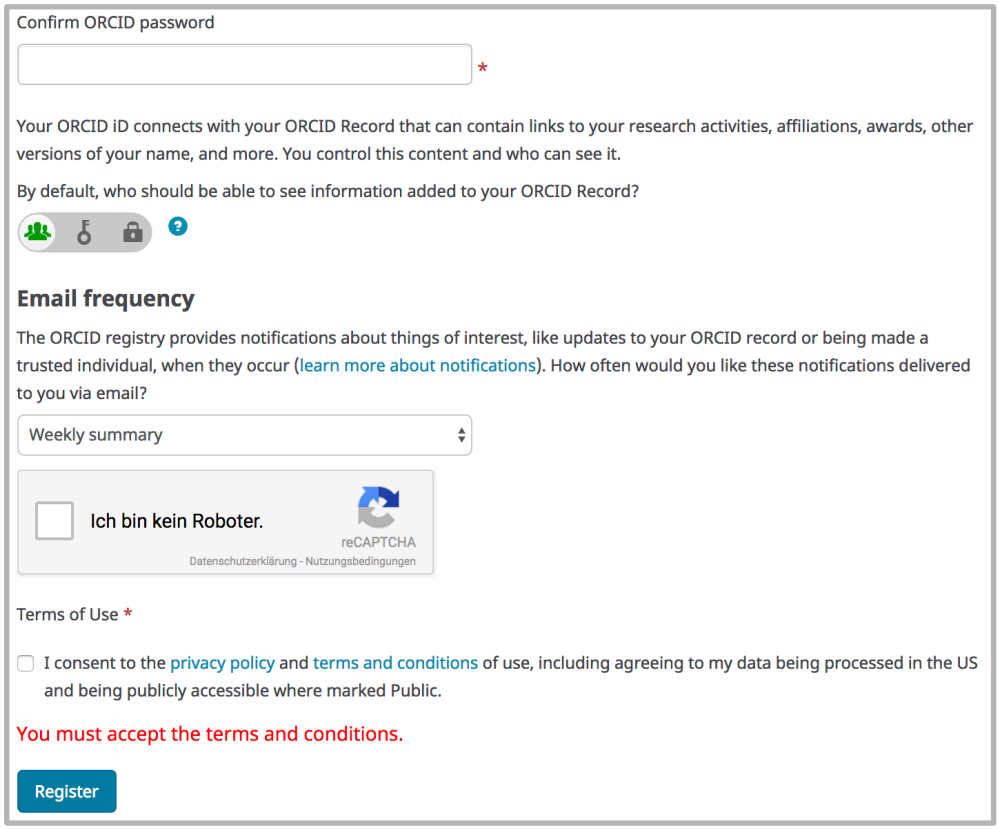

Abbildung 3: Einverständnismechanismus

2. Erstellung und Bearbeitung des ORCID-Profils

Die Erstellung und Bearbeitung der im ORCID-Profil gespeicherten Informationen stellen eine zentrale Funktion von ORCID dar. Im Folgenden wird dabei einerseits zwischen den Informationen unterschieden, die hinzugefügt und bearbeitet werden können, und andererseits zwischen den Personen, die einzelne Informationen hinzufügen und bearbeiten dürfen.

[22] Siehe unter https://orcid.org/register.

a) Datenkategorien

Das Portal stellt den Nutzerinnen und Nutzerinnen folgende Datenkategorien zur Verfügung. Damit können sie Informationen über sich und ihre wissenschaftliche Tätigkeit verwalten, wie zum Beispiel öffentlich machen.

Dazu gehören zunächst allgemeine Angaben zur Person, insbesondere:

- weitere eindeutige Kennungen wie zum Beispiel ResearcherID;
- weitere Namensformen, die der Wissenschaftler oder die Wissenschaftlerin in Zusammenhang mit seiner oder ihrer wissenschaftlichen Tätigkeit verwendet;
- Schlüsselwörter, mit Hilfe derer er oder sie von anderen aufgefunden und identifiziert werden möchte;
- externe Internetseiten, etwa diejenige seines oder ihres persönlichen Blogs oder aktuellen Arbeitgebers;
- weitere E-Mail-Adressen.

Darüber hinaus gehören dazu weitere spezifische Angaben, insbesondere:

- zur Biographie (im Folgenden „Biography“);
- zur Ausbildung (im Folgenden „Education“);
- zu vorangegangenen und aktuellen Anstellungen (im Folgenden: „Employment“);
- Förderungen (im Folgenden: „Funding“) und
- wissenschaftlichen Arbeiten (im Folgenden: „Works“).

Die Nutzerinnen und Nutzer können diese Angaben je nach Themenbereich manuell, halbautomatisiert oder vollautomatisiert in das System einpflegen. Sie können wissenschaftliche Arbeiten auch über Verlinkungen zu Internetseiten von ORCID-Partnern („search and link“) und vollautomatisiert über ein Importprogramm für BibTex-Dateien einspeisen.[23] Die Wissenschaftlerin oder der Wissenschaftler kann diese Angaben zu jedem Zeitpunkt löschen, ändern oder weitere Angaben hinzufügen.[24]

b) Privacy-Funktionalität: Spezifische Einstellungen

Je nach zuvor beschriebener Privacy-Voreinstellung stehen alle Angaben grundsätzlich entweder nur dem Nutzer oder der Nutzerin, nur bestimmten

[23] Siehe die Übersicht unter http://support.orcid.org/knowledgebase/topics/32827-using-the-orcid-registry.
[24] Siehe insbesondere unter Punkt 8.0 Privacy Policy.

„trusted parties“ oder der Allgemeinheit öffentlich zur Verfügung (siehe Abbildung 4).

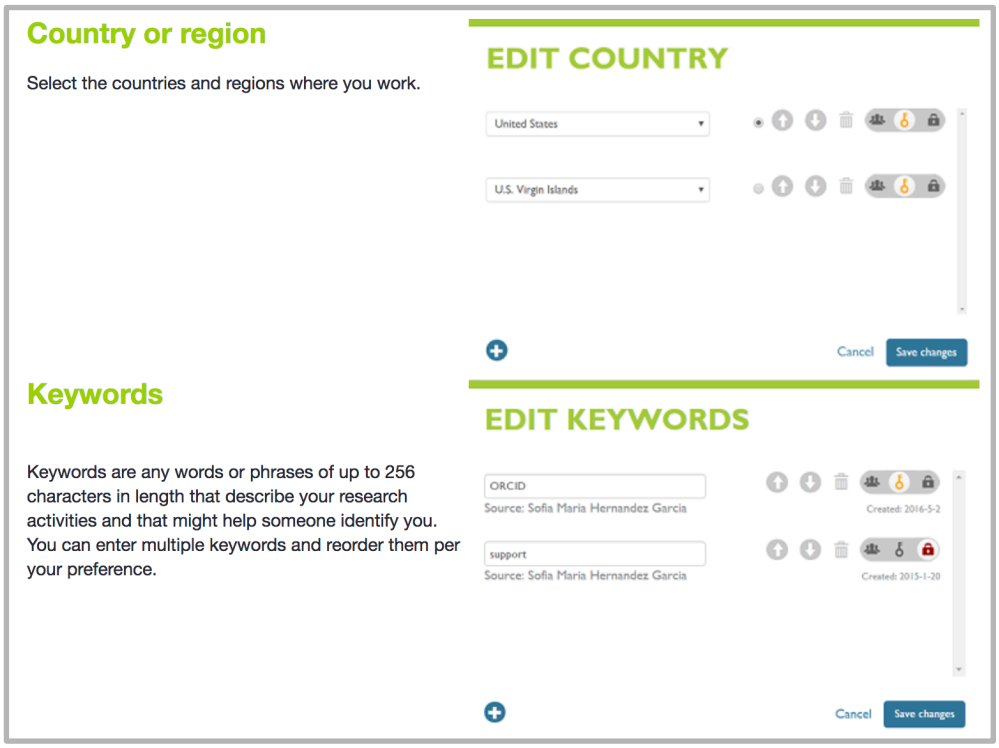

Abbildung 4: weitere Einstellungen

Nutzerinnen und Nutzer können darüber hinaus jede Einzelangabe innerhalb dieser Bereiche (zum Beispiel eine bestimmte E-Mail-Adresse, berufliche Stelle oder wissenschaftliche Arbeit) anpassen, also entweder als „public“, „private“ oder „limited access“ kennzeichnen.[25] Über eine „bulk edit“-Funktion, können die Einstellungen auch komfortabel in einem Durchgang für mehrere ausgewählte Publikationen geändert werden.[26]

c) Delegation der Verwaltung an „Trusted Parties“

Wissenschaftlerinnen und Wissenschaftler können auch andere Personen zumindest teilweise mit der Verwaltung ihres ORCID-Profils betrauen, nämlich die sogenannten „Trusted Parties“. Im Folgenden wird hierbei unterschieden zwi-

[25] Siehe zum Beispiel unter http://support.orcid.org/knowledgebase/articles/187920-add-personal-information-to-your-orcid-record.
[26] Vgl. http://support.orcid.org/knowledgebase/articles/462032#Edit.

schen vertrauenswürdigen Einzelpersonen („Trusted Individuals“) und vertrauenswürdigen Organisationen („Trusted Organizations“).

„Trusted Individuals“ können für die registrierte Nutzerin beziehungsweise für den registrierten Nutzer das jeweilige ORCID-Profil verwalten. Eine solche vertrauenswürdige Einzelperson kann keine elementaren Veränderungen des ORCID-Profils vornehmen, wie zum Beispiel das Passwort ändern, E-Mail-Adressen entfernen oder weitere vertrauenswürdige Personen hinzufügen, ebenso wenig kann sie die Einstellungen zur Datensicherheit einsehen oder verändern. Sie erhält aber vollen Einblick in die sonstigen Angaben, inklusive derer, die als „private“ gekennzeichnet wurden und somit nur dem Nutzer oder der Nutzerin selbst zur Verfügung stehen. Die vertrauenswürdige Einzelperson kann diese Angaben ändern, neue Angaben hinzufügen, die entsprechenden Privacy-Einstellungen vornehmen sowie weitere vertrauenswürdige Organisationen benennen. Der Wissenschaftler oder die Wissenschaftlerin kann in den Einstellungen des ORCID-Profils jederzeit vertrauenswürdigen Einzelpersonen den Zugang entziehen, aber auch weitere „Trusted Individuals“ benennen.[27]

„Trusted Organizations“ sind solche Organisationen, denen Nutzerinnen und Nutzer oder berechtigte Einzelpersonen bestimmte Zugangs- und/oder Verwaltungsrechte eingeräumt haben. Zum Beispiel kann ein Verlag autorisiert werden, dem ORCID-Profil Informationen über die wissenschaftlichen Arbeiten der Wissenschaftlerin oder des Wissenschaftler hinzuzufügen, oder eine wissenschaftliche Fördereinrichtung kann das Recht erhalten, Informationen über wissenschaftliche Arbeiten des Wissenschaftlers oder der Wissenschaftlerin einzusehen. Diese Rechte können entweder für einen Einzelfall oder solange eingeräumt werden, bis der Wissenschaftler oder die Wissenschaftlerin (oder eine vertrauenswürdige Einzelperson) diese widerruft. Wenn eine Organisation Informationen über eine Wissenschaftlerin oder einen Wissenschaftler ihrem oder seinem ORCID-Profil hinzufügen möchte, ohne dazu autorisiert, sprich, als vertrauenswürdig benannt zu sein, kann sie sich an ORCID wenden. ORCID wiederum fragt bei der betreffenden Wissenschaftlerin oder Wissenschaftler an, ob er oder sie die entsprechenden Verwaltungsrechte freigeben möchte.[28]

3. Nutzung der im ORCID-Profil gespeicherten Daten

Im Folgenden werden verschiedene Nutzungsszenarien der im ORCID-Profil gespeicherten Informationen dargestellt. Dabei unterscheidet die Darstellung zwischen verschiedenen Informationen (insbesondere ob als „private“ oder

[27] Punkt 3.0, 4.3 und 7.1 Privacy Policy.
[28] Punkt 3.0 und 4.1.2 Privacy Policy.

„public“ gekennzeichnet), den Personen beziehungsweise Organisationen, die die Informationen nutzen möchten, und zwischen den Zwecken, für die die Informationen genutzt werden sollen.

a) Datennutzungsszenarien: ORCID

ORCID erhebt und verarbeitet sowohl die Registrierungs- und Profilangaben, die durch den Wissenschaftler oder die Wissenschaftlerin beziehungsweise seine „trusted parties“ eingegeben wurden, als auch die Nutzungsdaten, die beim Gebrauch der Webseite und des Systems anfallen (zum Beispiel die Auskunft darüber geben, wer wann bestimmte Angaben im ORCID-System macht). ORCID erhebt und verarbeitet diese Daten, um das technische System inklusive seiner Internetseiten entsprechend seinen Zielen zu betreiben: Wissenschaftlerinnen und Wissenschaftler global eindeutig zu identifizieren und ihnen Werke eindeutig zuordnen zu können. Hierzu zählt laut ORCIDs Privacy Policy auch die Datenverarbeitung zu folgenden Zwecken:

- Erbringung der technischen Dienste des ORCID-Registers sowie seine Instandhaltung, Evaluierung und Verbesserung. Laut den Angaben in ORCIDs Privacy Policy werden dafür auch Daten verarbeitet, die ein Wissenschaftler oder eine Wissenschaftlerin als „private“ oder „limited access“ kennzeichnet hat.[29]
- Diese Daten werden auch verarbeitet, insbesondere um eventuelle Konflikte bezüglich der Identität, Richtigkeit oder Herkunft bestimmter Angaben zu lösen.[30]
- Zur Lösung eines Konfliktes gibt ORCID schließlich die E-Mail-Adresse an die andere Konfliktpartei oder eine Streitbeilegungsinstanz weiter.[31]

Um diese Dienste zu erbringen beziehungsweise diese Zwecke zu erreichen, bedient sich ORCID verschiedener Dienstleister und Vertragspartner (zum Beispiel um Speicherplatz bereitzustellen). Diese sind verpflichtet, die Daten einzig zu den genannten Zwecken zu verwenden („need to know“) und die von ORCID geforderten Vertraulichkeits- und Datensicherheitsvorkehrungen zu treffen.[32]

ORCID nutzt die gespeicherten Daten unter anderem auch, um die Wissenschaftlerin oder den Wissenschaftler für die folgenden Zwecke zu kontaktieren:

- Um (wie zuvor bereits erwähnt) Anfragen einer Mitgliedsorganisation

[29] Punkt 6.0 Privacy Policy.
[30] Punkt 6.0 Privacy Policy.
[31] Punkt 7.1 Privacy Policy.
[32] Punkt 7.2 Privacy Policy.

von ORCID an die Wissenschaftlerin oder den Wissenschaftler weiterzureichen, die anfragen, sie als „trusted organization“ zu kennzeichnen;
- um die Wissenschaftlerin oder den Wissenschaftler über Änderungen der Datenschutzerklärung oder der Nutzungsvereinbarung von ORCID zu informieren, zum Beispiel Änderungen des Registrierungsprozesses, der Privacy-Funktionalität oder der jeweils erhobenen Daten;
- um der Wissenschaftlerin oder dem Wissenschaftler einen Newsletter mit Informationen über ORCID zuzusenden (dabei gibt es die Möglichkeit zum Opt-out).[33]

b) Datennutzungsszenarien: „Trusted parties“

Sogenannte „trusted parties“ erhalten nicht nur Einblick in die Angaben, die die Wissenschaftlerin oder der Wissenschaftler als „public“ gekennzeichnet hat, sondern auch in weitere Angaben. Wie bereits erwähnt, erhält eine als vertrauenswürdig gekennzeichnete Einzelperson („trusted individual“) vollen Einblick in sämtliche Angaben eines Profils, selbst in solche, die als „private“ gekennzeichnet sind (bis auf das Passwort und den Zugang zu Einstellungen der Datensicherheit).[34]

Vertrauenswürdige Organisationen erhalten Zugang über die öffentlich gemachten Informationen hinaus grundsätzlich nur zu den Angaben, die ihnen die Wissenschaftlerin oder der Wissenschaftler oder eine von ihr oder ihm als vertrauenswürdig bezeichnete Einzelperson im Rahmen der „limited access“-Einstellung zugänglich macht (dies geschieht in der Regel über eine eigens hierfür von ORCID bereit gestellte technische Schnittstelle). Vertrauenswürdige Organisationen können jedoch Angaben einsehen, die als „private“ gekennzeichnet wurden, wenn sie diese selbst erstellt haben.[35]

Die Mitgliedschaftsvereinbarung zwischen ORCID und der vertrauenswürdigen Organisation legt außerdem fest, dass sie Angaben, die als vertrauenswürdig gekennzeichnet sind, Dritten nicht zugänglich machen. Es bestehen jedoch zwei Ausnahmen:
- Erstens für den Fall, dass diese Daten bereits über eine anderen Quelle öffentlich zugänglich sind;
- zweitens, solange und soweit die vertrauenswürdige Organisation die Wissenschaftlerin oder den Wissenschaftler darüber informiert, an wen und wie sie die Informationen weitergeben möchte.[36]

---

[33] Punkt 6.0 Privacy Policy.
[34] Siehe oben unter Abschnitt 2 m.V.a. Punkt 3.0, 4.3 und 7.1 Privacy Policy.
[35] Punkt 4.1.2 und 7.1 Privacy Policy.
[36] Punkt 3.0 und 4.1.2 Privacy Policy.

Die Verwendung solcher Daten für Marketingzwecke ist ORCID-Partnern nur erlaubt, solange und soweit sie die betroffenen Wissenschaftlerinnen und Wissenschaftler die Möglichkeit zum Opt-out haben. Die Daten dürfen nicht für Junk- oder Spam-Mails oder ähnliche Kommunikationszwecke verwendet werden.[37]

c) Datennutzungsszenarien: „Public"

Als „public" gekennzeichnete Angaben können grundsätzlich von jedem Dritten eingesehen beziehungsweise über eine eigens hierfür zur Verfügung stehende technische Schnittstelle abgerufen und ausgewertet werden. Da der Zugang zu diesen Daten unter einer CC0-Lizenz[38] steht, findet keine ausdrückliche Zweckbegrenzung statt.[39] Nicht als „public" bezeichnete Daten werden nur in aggregierter Form verwendet, das heißt, in einer Weise, die die Identität der Wissenschaftlerin oder des Wissenschaftlers schützt, oder aufgrund gesetzlicher Verpflichtungen von ORCID.[40]

4. Weitere Funktionen

a) ORCID als Identitätsmanagementsystem für Authentifizierungszwecke (Single-Sign-on via ORCID)

Es gibt Überlegungen, ORCID zukünftig auch mit Funktionalitäten auszustatten, die es ermöglichen, über die ORCID iD auch Authentifizierungen gegenüber anderen Diensten vorzunehmen.[41] ORCID würde so zum „Identity Provider" gegenüber diesen anderen Diensten („relying parties"). Bisher gehören derartige Funktionen noch nicht zum bestehenden System und stellen keine Kernfunktionalität von ORCID dar. Daher wird die Funktion vorliegend nicht vertieft betrachtet.

---

[37] Punkt 7.3 Privacy Policy.

[38] CC0 bezeichnet „Creative Commons Zero", zur Kennzeichnung von Inhalten frei von Urheberrechten. Die Konstruktion ist dabei für Rechtsordnungen wie die Deutsche, in denen ein Verzicht auf eigenes Urheberrecht gesetzlich nicht möglich ist, dass eine Lizenz unter weitest möglichem Verzicht auf Urheberrechte eingeräumt wird (so genannte „Public License Fallback", vgl. https://creativecommons.org/publicdomain/zero/1.0/ (22.3.2016) bzw. den dort verlinkten Lizenztext unter Nr. 3.

[39] Punkt 7.1 und 7.3 Privacy Policy.

[40] Punkt 7.5 Privacy Policy.

[41] Siehe unter: https://github.com/ORCID.

b) Zukünftige Zwecke

Darüber hinaus sollen mögliche zukünftige Zwecke der Nutzung von im ORCID-Profil gespeicherten Daten untersucht und diskutiert werden. Denkbar wären zum Beispiel folgende Nutzungsszenarien:

- Neue Nutzungsformen der Daten durch Wissenschaftlerinnen und Wissenschaftler;
- neue Nutzungsformen der Daten durch Trusted Parties (zum Beispiel die Nutzung von ORCID für die eindeutige Identifizierung zum Zwecke der automatisierten Evaluation durch den Arbeitgeber) sowie
- neue Nutzungsformen der Daten durch Dritte (zum Beispiel die Nutzung von ORCID für die eindeutige Identifizierung zum Zwecke der automatisierten Evaluation durch Forschungsförderer).

5. Zusammenfassung

Die Darstellung dieses Kapitels folgte der Perspektive der Wissenschaftlerinnen und Wissenschaftler, die sich auf dem Portal ein Profil anlegen, Informationen über sich im Rahmen ihres Profils einpflegen und mit Blick auf die unterschiedlichen Nutzungsszenarien zur Verfügung stellen.

Im den folgenden Ausführungen sollen diese Nutzungsszenarien entsprechend der datenschutzrechtlichen Kategorien dargestellt werden. Diese Darstellung nach rechtlichen Kategorien ist erforderlich, um die jeweilige Datennutzung entsprechend ihrer datenschutzrechtlichen Relevanz prüfen zu können.

Zentrales Element für diese Kategorisierung stellen die Verwendungszwecke der verschiedenen Akteure dar, die wie in nachfolgender Tabelle 1 dargestellt, umrissen werden können.

Datenverarbeitende Stelle		
	Zweck	
		Datenkategorien
ORCID (eigene Zwecke)		
	Identifizierung und Zuordnung	
		Registrierungsdaten
		Profilangaben („public“, „limited access“, „private“)
		Nutzungsdaten
	Webseite (Instandhaltung, Evaluierung, Verbesserung)	
		Profilangaben („public“, „limited access“, „private“)
		Nutzungsdaten
	Kontaktherstellung (Subzwecke)	
		Kontaktanbahnung zwischen Nutzenden und Organisation
		Information über Änderungen der Nutzungsbedingungen bzw. der Privacy Policy
		Information über Marketingmaßnahmen (Newsletter verbunden mit Opt-out-Funktion)
Trusted Individuals		
	Zwecke durch die Nutzerinnen und Nutzer vorgegeben	
		Profilangaben („public“, „limited access“, „private“)
Trusted Organizations (eigene Zwecke, zum Teil vertraglich beschränkt durch ORCID, im Übrigen gesetzlich beschränkt)		
	Marketingzwecke (vertraglich beschränkt)	
		Profilangaben („public“, „limited access“, „private“)
	Weitergabe an Dritte (vertraglich beschränkt)	
		Profilangaben („public“, „limited access“)
Sonstige Dritte		
	unbeschränkte Zwecke (aber gesetzlich beschränkt)	
		Profilangaben („public“)

Tabelle 1: Datenverarbeitende Stellen, Zwecke und Datenkategorien

III. Allgemeine datenschutzrechtliche Erwägungen

Ziel der rechtlichen Untersuchung in diesem Abschnitt ist, eine datenschutzrechtliche Bewertung zentraler Funktionalitäten der ORCID-Plattform für Individuen und Organisationen in Deutschland durchzuführen. Hierfür sind derzeit die datenschutzrechtlichen Bestimmungen des deutschen Rechts, insbesondere des Bundesdatenschutzgesetzes (BDSG) einschlägig. Bei der folgenden Darstellung wird an entsprechender Stelle – wie eingangs bereits erwähnt – auch auf zugrunde liegende beziehungsweise die am 28. Mai 2018 in Kraft tretende EU-Datenschutz-Grundverordnung (im Folgenden: DSGVO) zurückgegriffen.

Bei dem untersuchten Angebot handelt es sich um einen elektronischen Informations- und Kommunikationsdienst. Es ist weder ein Telekommunikationsdienst noch ein telekommunikationsgestützter Dienst im Sinne des Telekommunikationsgesetzes noch Rundfunk im Sinne des Rundfunkstaatsvertrags. Es handelt sich also um einen Telemediendienst. Daher sind – sofern eine entsprechende Regelung besteht – auch die spezielleren Regelungen des Telemediengesetzes (TMG) zu beachten. Sie gehen den Regelungen des BDSG insoweit vor (*lex specialis*), § 1 Abs. 3 S. 1 BDSG.

Diese Regelungen werden mit In-Kraft-Treten der bereits verabschiedeten europäischen Datenschutzgrundverordnung[42], DSGVO, im Mai 2018 sowie der derzeit erst im Entwurf vorliegenden ePrivacy-Verordnung weitgehend ersetzt. Anders als die EU-Vorgängerregelungen, die als Richtlinien verabschiedet wurden, die einer Umsetzung durch nationale Gesetze bedurften, sind die Novellierungen Verordnungen und gelten damit unmittelbar. Trotzdem sind an einer Reihe von Stellen durch den nationalen Gesetzgeber Präzisierungen und Ausnahmen möglich oder erforderlich (so insbesondere im Rahmen von Art. 89 DSGVO für wissenschaftliche Zwecke im öffentlichen Interesse). In Deutschland liegt in Hinblick auf die DSGVO bisher lediglich ein Referentenentwurf vor, bezüglich der ePrivacy-Verordnung ist noch nicht abzusehen, ob und inwieweit ein etwaiger nationaler Umsetzungsspielraum besteht und genutzt werden wird.

Anknüpfungspunkt ist für die hier gemachten Betrachtungen das derzeit geltende Datenschutzrecht. Bisher gibt es nur wenige Anhaltspunkte, dass sich durch die Novellierungen die rechtliche Bewertung im Ergebnis fundamental ändern würde. Wo Auswirkungen bereits erkennbar sind, ist dies im Text erwähnt.

---

[42] Verordnung (EU) 2016/679 vom 27. April 2016, http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.DEU&toc=OJ:L:2016:119:TOC.

In der nun folgenden allgemeinen Prüfung der datenschutzrechtlichen Zulässigkeit der im Untersuchungsgegenstand beschriebenen Verarbeitung, soll zunächst der Anwendungsbereich (1.) und der Regelungsadressat (2.) herausgearbeitet werden, um sodann anhand grundlegender datenschutzrechtlicher Prinzipien der Rechtmäßigkeit (3.), der Zweckbindung und Erforderlichkeit (4.) sowie der flankierenden Anforderungen der Transparenz, (Daten-)Sicherheit und Kontrolle (5.) eine erste rechtliche Einordnung der Plattform zu ermöglichen.

Zu beachten ist dabei, dass das Datenschutzrecht oft einen breiten Interpretationsspielraum zulässt und keine höchstrichterliche Rechtsprechung zu einer Vielzahl von Rechtsfragen besteht. Die rechtliche Beurteilung kann daher nicht immer verlässlich gewährleistet werden, sondern lediglich rechtliche Risiken aufzeigen. Orientierung geben in diesen Fällen neben den klassischen juristischen Auslegungsmethoden insbesondere die Stellungnahmen von Aufsichtsbehörden sowie die einschlägige Literatur.

1. Anwendungsbereich: Personenbezogene Daten

Datenschutzrecht wird immer dort relevant, wo eine Verarbeitung personenbezogener Daten stattfindet.[43] Personenbezogene Daten sind dabei nicht nur solche Angaben über natürliche Personen, bei denen offensichtlich ist, wem diese Angaben zuzuordnen sind. Vielmehr reicht es aus, dass die Möglichkeit besteht, dass eine solche Zuordnung durchgeführt werden kann („bestimmbare natürliche Person", § 3 Abs. 1 BDSG). Ausschlaggebend für die Bestimmbarkeit ist dabei nicht nur das Wissen der Einrichtung, die die Daten verarbeitet (im folgenden „datenverarbeitende Stelle"). Es kann bereits ausreichend sein, dass die Identität im Zusammenspiel mit Dritten bestimmt werden kann.[44]

a) Registrierungs-, Profil- und Nutzungsdaten der (eingeloggten) Profilnutzer

Bei den oben beschriebenen Registrierungs- und Profildaten handelt es sich zweifelsohne um personenbezogene Daten der Profilnutzerinnen und -nutzer, so dass diesbezüglich die datenschutzrechtlichen Vorschriften anwendbar sind.

---

[43] Ausgenommen sind lediglich rein private Nutzungen. § 1 Abs. 3 a.E. BDSG, Art. 2 Abs. 2 c) DSGVO, sog. „Household-Exemption".

[44] Vgl. etwa: Artikel-29-Gruppe, „Stellungnahme 4/2007 zum Begriff personenbezogener Daten", online: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_de.pdf (23.3.2017). Für dynamische IP-Adressen unlängst bestätigt durch EuGH Urt. v. 19.10.2016, Rs. C-582/14.

Darüber hinaus kommt das Datenschutzrecht auch in Hinsicht auf die sogenannten Nutzungsdaten zur Anwendung, die erhoben werden, wenn die Plattform lediglich rein lesend aufgerufen wird. Nutzungsdaten sind zum Beispiel Merkmale zur Identifikation einer Nutzerin oder eines Nutzers sowie Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung der Plattform, vgl. § 14 Abs. 1 S. 2 TMG. Dies ist offenkundig in den Fällen, in denen die (lesenden) Nutzerinnen und Nutzer auf der Plattform eingeloggt sind, da hier die Nutzungsdaten durch die Verknüpfung mit dem registrierten Profil dem Profilnutzer eindeutig zugeordnet werden können.[45]

b) Nutzungsdaten nicht eingeloggter Portalnutzer

Das kann aber auch dann der Fall sein, wenn eine Nutzung durch nicht eingeloggte Dritte stattfindet, da notwendigerweise zumindest deren IP-Adressen verarbeitet werden. Derzeit ist noch nicht abschließend geklärt, in welchen Fällen eine Speicherung und Weiterverarbeitung dieser Nutzungsdaten zulässig ist.[46] Ob die Datenverarbeitung insofern dem Datenschutzrecht hinreichend entspricht, kann daher nicht abschließend entschieden werden. Zur Risikominimierung könnte es sich daher empfehlen, die Verarbeitung von IP-Adressen auf ein Mindestmaß zu beschränken, also etwaige Zugriffsprotokolle unmittelbar nach dem Zugriff zu löschen oder zumindest die IP-Adressen zu entfernen, in der Hoffnung, dass so eine hinreichende Anonymisierung erreicht werden kann.

c) Zuordnung anonymisierter Nutzungsdaten zu Profilinhabern

Hierbei ist zu beachten, dass die aus den Zugriffen abgeleitete Information (zum Beispiel wie oft ein einzelnes Profil aufgerufen wird) ein personenbezogenes Datum des *Profilinhabers* darstellt, selbst wenn die Zugriffsdaten der *Leser* der Plattform erfolgreich anonymisiert wurden. Ob und in welchem Umfang derartige Analysen durchgeführt werden oder geplant sind, ist aus der Datenschutzerklärung nicht mit hinreichender Deutlichkeit zu erkennen, so dass eine Bewertung nicht möglich ist.

d) Anonymisierung personenbezogener Daten

Grundsätzlich ist festzuhalten, dass Grenzfälle zur Anwendung des Datenschutzrechtes regelmäßig dann gegeben sind, wenn Daten etwa durch Aggre-

[45] Vgl. EuGH C-70/10 sowie EuGH C-360/10.
[46] Siehe o.g. Entscheidung des EuGH und zugrundeliegender Rechtsstreit beim BGH, a.a.O.

gation anonymisiert sind. Sofern die Daten wirksam anonymisiert sind, entfällt der Personenbezug und Datenschutzrecht ist nicht mehr anwendbar. Allerdings führt eine wirksame Anonymisierung im Regelfall dazu, dass jegliche inhaltliche Aussage verloren geht; andernfalls besteht regelmäßig ein erhebliches Re-Identifikationsrisiko. Dies könnte auch für die oben bereits beschriebenen Auswertungen aggregierter Datenbestände bestehen, so dass sich hier eine sorgfältige Untersuchung der Anonymisierungsmechanismen empfiehlt. Für die weitere Betrachtung soll unterstellt werden, dass die Daten – wie in der Datenschutzerklärung der Plattform angegeben – erfolgreich und vollständig anonymisiert wurden, so dass datenschutzrechtliche Vorschriften außer Betracht bleiben können.

e) Zwischenfazit

Auf ORCID werden verschiedene Arten personenbezogener Daten verarbeitet, wobei den Datenbeständen der Nutzerinnen und Nutzern wohl die größte Bedeutung zukommt. Gegenstand der weiteren Betrachtung ist daher insbesondere der Datenbestand der Nutzerinnen und Nutzer des ORCID-Portals entlang der Kategorien Registrierungs-, Profil- und Nutzungsdaten.

2. Regelungsadressat: Verantwortliche Stelle

Das Datenschutzrecht adressiert und verpflichtet die für die Datenverarbeitung verantwortliche Stelle (datenverarbeitende Stelle) und ihre Auftragnehmer (Auftragsdatenverarbeiter). Die datenverarbeitende Stelle ist die Einrichtung, die personenbezogene Daten erhebt, verarbeitet oder nutzt, § 3 Abs. 7, sofern sie nicht Auftragsdatenverarbeiter gem. § 11 BDSG ist. Nach der dem BDSG zugrunde liegenden EU-Datenschutzrichtlinie 94/96/EG (im Folgenden: RL 95/46, dort: Art. 2 lit. d) sowie der im Mai 2018 endgültig in Kraft tretenden DSGVO (Art. 4 Nr. 7) ist verantwortliche Stelle „die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“. Demgegenüber ist gem. Art. 2 lit. e RL 95/46 bzw. Art. 4 Nr. 8 DSGVO Auftragsdatenverarbeiter, „eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet“.

a) ORCID als datenschutzrechtlich verantwortliche Stelle

In der zunächst betrachteten Fallkonstellation, in der die Wissenschaftlerinnen und Wissenschaftler ihr Profil eigenständig und im eigenen Interesse anlegen und pflegen, ist nach beiden Definitionen ORCID als datenverarbeitende und damit auch verantwortliche Stelle anzusehen. Dies gilt sowohl für die unter-

schiedlichen Datenkategorien als auch die unterschiedlichen Zwecke, zu denen ORCID die Verarbeitung dieser Daten vornimmt. Dabei wird im Folgenden grundsätzlich zwischen den folgenden Verarbeitungszwecken von ORCID unterschieden:

- ORCID erhebt und verarbeitet Registrierungs-, Profil- und Nutzungsdaten von Profilnutzerinnen und -nutzern zunächst, um ihre weltweit eindeutige Identifizierung im wissenschaftlichen System sowie die Zuordnung ihrer wissenschaftlichen Werke zu ermöglichen.
- Dabei erhebt und verarbeitet ORCID diese Daten insbesondere, um das Portal instand zu halten, zu evaluieren und zu verbessern sowie
- um die Nutzer zu kontaktieren, beispielsweise um sie auf Änderungen der Privacy Policy aufmerksam zu machen, um einen Kontakt mit weiteren Teilnehmenden des wissenschaftlichen Systems herzustellen oder für eigene Marketingmaßnahmen.

ORCID ist lediglich dann nicht für die Datenverarbeitung verantwortlich, wenn ORCID die Daten nicht zu eigenen Zwecken erhebt und verarbeitet, sondern im Auftrag eines Dritten handelt und sich an von diesem vorgegebene Zwecke hält. Dies könnte etwa der Fall sein, wenn ORCID die Daten im Auftrag eines Arbeitgebers einer Nutzerin oder eines Nutzers verarbeitet.

Abgesehen von solchen Fällen der Auftragsdatenverarbeitung, spielt es für die Anwendung der datenschutzrechtlichen Vorschriften keine Rolle, dass die Betreiberfirma ORCID Inc. ihren Sitz in den Vereinigten Staaten von Amerika hat. Das Datenschutzrecht ist nach § 1 Abs. 5 Satz 2 BDSG auch für im Ausland gelegene Stellen anwendbar, da es ausschließlich auf die Erhebung im Inland (also in Deutschland) abstellt, was die für die hier untersuchten Fallkonstellationen unterstellt wird. Anders wäre der Fall nach der vorgenannten Norm nur zu beurteilen, wenn es sich um eine Entität mit einem Sitz in einem anderen Sitz der Europäischen Union oder in einem anderen Vertragsstaat des Europäischen Wirtschaftsraumes handeln würde. In jedem Fall wird nach Art. 3 DSGVO auch die Datenschutz-Grundverordnung mit ihrem Inkrafttreten auf die hier beschriebene Datenverarbeitung anwendbar sein.

b) Verantwortlichkeit weiterer Verwender der Daten

Neben ORCID (sowie einem gegebenenfalls in Erscheinung tretenden Auftraggeber) gibt es allerdings noch weitere Akteure des wissenschaftlichen Systems, die als datenschutzrechtlich verantwortliche Stelle in Betracht kommen können.

Entsprechend der vorgehenden Darstellung der Nutzungsszenarien könnte dies zunächst für die schon genannten Trusted Individuals gelten. Allerdings werden diese allein aufgrund Weisung des jeweiligen Profilinhabers tätig, mithin nur zu mit diesem vereinbarten Zwecken, und nutzen dabei lediglich die durch das Portal zur Verfügung stehenden Mittel. Deshalb sind diese nach der vorstehenden Definition keine datenschutzrechtlich verantwortliche Stelle.

Als verantwortliche Stelle kommen allerdings die Trusted Organizations in Betracht. Diese können insbesondere auf solche Daten zugreifen, die Nutzer von ORCID ihnen unter „limited access" zur Verfügung gestellt haben. Es liegen zwar keine umfassenden Angaben darüber vor, zu welchen Zwecken Trusted Organizations diese Daten nutzen. Insbesondere kann nicht abschließend geklärt werden, ob eine solche Nutzung aufgrund eigener Zwecksetzung oder aufgrund Weisung eines weiteren Dritten erfolgt. ORCIDs Privacy Policy lässt aber vermuten, dass zumindest eine Datenverarbeitung zu eigenen Marketingzwecken in Betracht gezogen werden kann. Insoweit verarbeiten Trusted Organizations die Daten zu eigenen Zwecken und sind datenschutzrechtlich die verantwortliche Stelle. Auch nennt ORCIDs Privacy Policy den Fall, dass Trusted Organizations die Daten an Dritte weitergeben. Sofern dies aufgrund eigener Zwecksetzung beruht, sind sie auch hier die verantwortliche Stelle.

Schließlich stehen die personenbezogenen Daten, die eine Nutzerin oder ein Nutzer von ORCID „public" gemacht hat, jedermann zur Verfügung, sprich, allen Personen ohne Beschränkung. Auch hier kommt grundsätzlich eine datenschutzrechtliche Verantwortlichkeit in Betracht. Hierbei gibt es allerdings keine Anhaltspunkte, ob diese Personen die öffentlich zur Verfügung gestellten Daten aufgrund eigener Zwecksetzung verarbeiten. Vorliegend können entsprechend keine Aussagen darüber gemacht werden, ob solche Verwendungen der Daten datenschutzrechtlich zulässig sind. Grundsätzlich gilt aber, dass die automatisierte Verarbeitung bereits öffentlich zugänglicher Daten rechtlich privilegiert wird. An sie werden also oftmals geringere Anforderungen gestellt als an die Verarbeitung noch nicht öffentlich zugänglich gemachter Daten. Im Fall einer rein privaten Nutzung könnte sogar die Anwendbarkeit datenschutzrechtlicher Vorschriften gänzlich entfallen.[47]

c) Zwischenfazit

Im Folgenden liegt der Schwerpunkt der Untersuchung daher auf Datenverarbeitungen, die durch ORCID selbst vorgenommen werden. Soweit es die vorliegenden Informationen zulassen, wird außerdem auf Datenverarbeitungen

[47] Wegen der „household-exemption", siehe oben.

durch „Trusted Organizations“ sowie am Rande durch sonstige Dritte eingegangen.

3. Rechtmäßigkeit, insbesondere Einwilligung

Die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten ist nur zulässig, sofern eine gesetzliche Grundlage besteht oder eine Einwilligung vorliegt, vgl. § 4 Abs. 1 BDSG (entsprechendes gilt nach Art. 6 Abs. 1 DSGVO).

a) Grundsätzliche Anforderungen an die Einwilligung

Als gesetzliche Grundlagen kommen vorliegend vor allem die gesetzlichen Erlaubnistatbestände des BDSG selbst sowie die des TMG in Betracht. Nach der vorherrschenden Ansicht in der rechtswissenschaftlichen Literatur ist für Bestands- und Nutzungsdaten auf das TMG anwendbar für die Inhaltsdaten das BDSG, wobei die Abgrenzung dieser Datenarten nicht immer ganz trivial ist.[48] Ein Rückgriff auf die jeweils enthaltenen gesetzlichen Erlaubnistatbestände ist jedoch dann nicht erforderlich, wenn eine wirksame Einwilligung der von der Datenverarbeitung betroffenen Personen (die Betroffenen) vorliegt. Die Einwilligung ist nach derzeitiger Rechtslage auch wirksam, wenn sie gegenüber einer datenverarbeitenden Stelle in einem Drittland erfolgt.[49]

Nach § 4a BDSG ist „die Einwilligung [...] nur wirksam,

- wenn sie auf der freien Entscheidung des Betroffenen beruht“,
- auf den „vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie,
- soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen des Betroffenen, auf die Folgen der Verweigerung der Einwilligung“ hingewiesen wird.
- Zudem bedarf die Einwilligung der Schriftform, „soweit nicht wegen besonderer Umstände eine andere Form angemessen ist“ (Hervorhebung durch Spiegelstriche im vorangegangenen und nachfolgenden jeweils durch die Verfasser)

§ 13 Abs. 2 TMG schreibt für die Einwilligung Spezialregelungen vor, nach denen „die Einwilligung [...] elektronisch erklärt werden [kann], wenn der Diensteanbieter sicherstellt, dass

---

[48] Spindler/Schuster (Spindler/Nink), Recht der elektronischen Medien, 3. Auflage 2015, § 15, Rn 3 und 7.

[49] Thomas Helbig, „Neue Regeln für Verträge mit Datenverarbeitern ausserhalb der EU“, in: Risk, Compliance & Audit" (Heft 3/2010, Seiten 29-33), gekürzt online: https://www.thomashelbing.com/de/neue-regeln-fuer-vertraege-datenverarbeitern-ausserhalb-eu (23.3.2017).

- der Nutzer oder die Nutzerin seine bzw. ihre Einwilligung bewusst und eindeutig erteilt hat,
- die Einwilligung protokolliert wird,
- der Nutzer den Inhalt der Einwilligung jederzeit abrufen kann und
- der Nutzer die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann."

b) Abgabe der Einwilligung durch Opt-in-Verfahren

Die Voraussetzungen für eine wirksame Einwilligung für die Datenverarbeitung von ORCID sind grundsätzlich für die oben dargestellten Registrierungs-, Profil- und Nutzungsdaten gegeben:

- Soweit die Regelungen des § 13 Abs. 2 TMG Vorrang haben, kann auf die nach dem BDSG vorgesehene Schriftform verzichtet werden. Eine elektronische Einwilligung - wie im Portal vorgesehen – ist zulässig. Soweit das BDSG anwendbar ist, wird man ebenfalls die elektronische Form für zulässig erachten müssen. Denn die Nutzerinnen und Nutzer müssten anderenfalls für einen aus ihrer Sicht einheitlichen Nutzungsvorgang zwei verschiedene Einwilligungen abgeben (etwa elektronisch, sprich, per Mausklick, für die Registrierungsdaten und für die Daten, die unmittelbar bei der Nutzung entstehen sowie schriftlich, sprich, per Post, für die Profildaten, also etwa die Daten über die verschiedenen Publikationen und etwaige biographischen Angaben). Auch lassen sich vorliegend keine Umstände für ein erhöhtes Schutzbedürfnis erkennen (etwa dass die Profildaten gegenüber den Registrierungs- und Nutzungsdaten schutzbedürftiger sind), die einen solchen Medienbruch von der elektronischen Form zur schriftlichen Form der Einwilligung erforderlich machen würden. Daher wird hier von „besonderen Umständen" ausgegangen, die ein Abweichen vom Schriftformerfordernis des BDSG erlaubten. Im Übrigen entspräche einem solch erhöhten Schutzbedürfnis auch die Privacy-Funktionalität (dazu sogleich).

- Die Protokollierung der Erklärung in elektronischer Form lässt sich ebenfalls sicherstellen und wird hier unterstellt.[50]

- Die Einwilligungserklärung ist hinreichend eindeutig formuliert; die Abgabe der Erklärung erfolgt bewusst. Sie wird zunächst bei der Registrierung über ein Opt-in-Verfahren („Checkbox") gewährleistet, in dessen

[50] Nach Auskunft der Betreiber findet eine Protokollierung der Registrierung und damit auch der Einwilligung statt.

Rahmen über einen Link auf die Privacy Policy auch die Funktionsweise des Portals erläutert wird, so dass die Zwecke der Verarbeitung grundsätzlich deutlich werden (siehe hierzu im Detail oben unter Teil III. 1.).

Schließlich ist zu berücksichtigen, dass die „Default"-Einstellung auf „public" steht.[51] Dies steht zwar einer wirksamen Einwilligung nicht unbedingt im Wege, könnte aber den Regelungen der ab März 2018 wirksamen DSGVO widersprechen, die in Art. 25 das Prinzip des „Privacy by Default" vorschreibt. Entsprechend ist zu überlegen, ob man die Änderung von „private" auf „public" den Nutzerinnen und Nutzern überlässt.

c) Weitere Transparenz- und Kontrollmechanismen durch die Privacy-Funktionalitäten

Für die Profilangaben können die Nutzerinnen und Nutzer über die Abgabe der elektronischen Einwilligung hinaus bei der Registrierung eine Voreinstellung vornehmen, ob die Daten der Öffentlichkeit, nur der Nutzerin oder dem Nutzer selbst oder einem anderen eingeschränkten Kreis von Personen zugänglich gemacht werden sollen.[52] Schließlich kann beim Erstellen jedes weiteren Eintrags noch einmal einzeln über den Adressatenkreis entschieden werden, worin jeweils eine erneute Einwilligung gesehen werden kann. Damit haben die Nutzerinnen und Nutzer innerhalb des Portals

- einen Überblick, welche Daten eingestellt wurden und
- können spezifisch für einzelne Datensätze den Adressatenkreis nachträglich anpassen oder Daten modifizieren und wieder entfernen.

Somit ist auch der jeweils gültige Inhalt dieser Einwilligung(en) transparent und widerruflich. Diese Umsetzung ist vorbildlich.

d) Freiwilligkeit der Einwilligung in besonderen Fallkonstellationen (insbesondere: Darstellung zur Rechtslage im Kontext des Datentransfers in die Vereinigten Staaten von Amerika)

Im Normalfall dürfte auch die Anforderung der Freiwilligkeit unproblematisch erfüllt sein. Probleme kann dieses Kriterium aufwerfen, wenn ein Arbeitgeber die Nutzung von ORCID vorschreibt. Da für wissenschaftliche Karrieren derzeit nach wie vor unabdingbar ist, in einschlägigen Fachverlagen zu publizieren, könnte auch eine von den Verlagen geforderte Registrierung (oder genauer:

[51] Siehe oben, Abbildung 2 und die zugehörigen Ausführungen.
[52] Hierdurch dürfte auch bereits die weitergehenden Anforderungen des Artikel 25 Abs. 2 DSGVO, der datenschutzfreundliche Voreinstellungen vorschreibt, Rechnung getragen werden.

die Angabe einer ORCID iD, was eine Registrierung voraussetzt) Zweifel an der Freiwilligkeit aufkommen lassen. Sofern solche Zwänge nicht existieren, ist jedoch davon auszugehen, dass die Einwilligung freiwillig erfolgt. Zu Berücksichtigen ist jedoch, dass bereits jetzt fast alle wissenschaftliche Einrichtungen im Rahmen ihres Informationsmanagements Angaben, wie z. B. Publikationen und Projekte, erfassen, so dass die in ORCID gespeicherten Informationen auch an anderen Stellen – häufig auch frei im Internet – zu finden sind.

Anders ist der Fall, wenn ein Arbeitgeber die Einrichtung einer ORCID iD verlangt. Dabei kommt es nicht darauf an, dass eine ausdrückliche Anweisung erfolgt. Aufgrund des Machtgefälles zwischen Arbeitnehmer und Arbeitgeber, ist davon auszugehen, dass eine Freiwilligkeit bereits dann nicht mehr unterstellt werden kann, wenn eine Teilnahme an der Plattform unausgesprochen erwartet wird. Die Rechtsgrundlage kann in diesen Fälle entweder der jeweilige Arbeitsvertrag, die – ggf. mit dem Betriebsrat abzustimmende – betriebliche Praxis oder das berechtigte Interesse des Arbeitgebers darstellen. In all diesen Fällen ist die Datenverarbeitung damit aber der entsprechenden Einrichtung zuzuordnen. Sie wird damit verantwortliche Stelle für die Datenverarbeitung. Da sie die Datenverarbeitung nicht selber durchführt, kann diese dann nur auf die Vorschriften zur Auftragsdatenverarbeitung nach § 11 BDSG gestützt werden. Allerdings müssen dann die dort beschriebenen Anforderungen erfüllt sein. Hierfür ist insbesondere nach Absatz 2 ein schriftlicher Auftrag (Auftragsdatenvereinbarung) an ORCID zu erteilen, der die weiteren in Absatz 2 näher aufgelisteten Anforderungen zu berücksichtigen hat. Daneben existiert eine regelmäßige Kontrollpflicht bezüglich der technisch-organisatorischen Maßnahmen und eine dementsprechende Dokumentationspflicht.

In der Praxis werden diese aufgelisteten Anforderungen regelmäßig auf der Basis von standardisierte Musterverträge realisiert, entsprechende Vorlagen werden unter anderem von Datenschutzaufsichtsbehörden angeboten.[53] Es ist zur Vereinfachung zu empfehlen, dass ORCID ein angepasstes Muster vorhält und entsprechenden Einrichtungen als Grundlage für den Abschluss einer Auftragsdatenvereinbarung anbietet.[54]

---

[53] Der Hessische Datenschutzbeauftragte (Hrsg.), „Mustervereinbarung für Auftragsdatenverarbeitung nach § 11 BDSG", https://www.datenschutz.hessen.de/download.php?download_ID=239 (7.5.2017) oder auch im Datenschutz-Wiki, vormals betrieben durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI), nunmehr gemeinsam von der Ruhr-Universität Bochum (RUB) und dem Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V., dort unter https://www.datenschutz-wiki.de/Mustervereinbarung_Auftragsdatenverarbeitung (7.5.2017).

[54] Ein ähnliches Vorgehen wählt etwa unter anderem die Google Inc. für die Durchführung ihres Dienstes Google Analytics, vgl. https://static.googleusercontent.com/media/www.google.de/de/de/analytics/terms/de.pdf (7.5.2017).

Die Kontrollmaßnahmen bezüglich der technisch-organisatorischen Maßnahmen müssen im Normalfall durch die Auftraggeber selbst, hier also die Arbeitgeber der Wissenschaftlerin oder des Wissenschaftlers, vorgenommen werden. Allerdings ist anerkannt, dass diese auch auf Basis einer geeigneten Auditierung durch Dritte vorgenommen werden können. Eine solche Auditierung kann insbesondere dann eine persönliche Kontrolle durch den Auftraggeber selbst ersetzen, wenn sie auf ein Zertifikat nach ISO/IEC 27001:2013 *Information technology – Security techniques – Information security management systems – Requirements* gestützt wird.[55]

Vorliegend ist schließlich zu berücksichtigen, dass die Datenverarbeitung im Auftrag nicht in einem EU-Mitgliedsstaat durchgeführt wird. Gem. § 4b Abs. 2 BDSG hat eine Übermittlung an Stellen, die nicht in Abs. 1 genannt sind (insbesondere nach Abs. 1 Nr. nicht in einem EU-Mitgliedsstaat belegen sind) „insbesondere" zu unterbleiben, wenn bei der Stelle ein angemessenes Schutzniveau nicht gewährleistet ist. Eine Vermutung für ein angemessenes Schutzniveau gilt dann, wenn die EU-Kommission einen entsprechenden „Angemessenheitsbeschluss" gem. Art. 25 Abs. 1 RL 95/46 gefällt hat. In Bezug auf Datenverarbeitungen in den Vereinigten Staaten besteht ein solcher Beschluss („EU-US Privacy-Shield").[56] Danach kommt „die Kommission zu dem Schluss, dass die Vereinigten Staaten ein angemessenes Schutzniveau für personenbezogene Daten gewährleisten, die im Rahmen des EU-US-Datenschutzschilds aus der Europäischen Union an selbstzertifizierte Organisationen." (Klausel 13 in der dt. Übersetzung, sic!).

Auch wenn in der deutschen Sprachfassung dem entsprechenden entscheidenden Satz das abschließende bedeutungstragende Verb fehlt, zeigt die englische Sprachfassung, aber auch die Auslegung, dass gemeint ist, dass nach den weiter ausgeführten Regeln selbstzertifizierte Organisationen ein angemessenes Schutzniveau erreichen.[57]

---

[55] wiederum Datenschutz-Wiki: https://www.datenschutz-wiki.de/Auftragsdatenverarbeitung (7.5.2017); Spindler/Schuster, "Recht der elektronischen Medien", 3. Auflage 2015, BDSG § 11, Rn 22. Allerdings wird in der Fachliteratur oft nicht hinreichend beachtet, dass dies nur dann gelten kann, wenn die entsprechende Zertifizierung auch mit einem umfassenden Untersuchungsgegenstand ("Scope") durchgeführt wird, vgl. ISO (Hrsg.), "ISO/IEC 27001:2013 *Information technology – Security techniques – Information security management systems – Requirements", S. 1, ("clause 4.3")*. Die Auditierung durch TRUSTe dürfte allerdings des Anforderungen nicht genügen, weil sie sich auf die Privacy Policy und nicht auf die technisch-organisatorischen Maßnahmen von ORCID bezieht.

[56] Europäische Kommission: Durchführungsbeschluss (EU) 2016/1250 der Kommission vom 12. Juli 2016 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes (Bekannt gegeben unter Aktenzeichen C(2016) 4176) (Text von Bedeutung für den EWR). In: *Amtsblatt der EU, ABl. L 207 vom 1. August 2016, S. 1–112.* Online: http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.DEU (26.5.2017).

[57] „concludes that the United States ensures an adequate level of protection for personal data transferred under the EU-U.S. Privacy Shield from the Union to self-certified organisations in the United States."

ORCID ist bestrebt, die Anforderungen an eine solche Selbstzertifizierung einzuhalten, sieht sich als Non-profit-Organisation aber von der Teilnahme an dem Programm ausgeschlossen, weil die für die Aufsicht über das Privacy Shield zuständige US-amerikanische Federal Trade Commission, keine Zuständigkeit für Non-Profits habe.[58] Entsprechend wird ORCID auch nicht auf der Liste der Federal Trade Commission geführt.[59] Damit gilt die Vermutung eines angemessenen Schutzniveaus auf Grundlage der erwähnten EU-Entscheidung für ORCID nicht.

Ob die Angemessenheit des Schutzniveaus dennoch erreicht ist kann nicht abschließend beurteilt werden. Zweifel bestehen insbesondere deswegen, weil die Selbstzertifzierung auch eine Versicherung für prozedurale Garantien – konkret die Unterwerfung unter eine Schiedsgerichtsbarkeit – vorsieht. Grundsätzlich enthält die Privacy Policy einen entsprechenden Hinweis auf eine Streitschlichtungsstelle.[60] Allerdings kann nicht eindeutig beurteilt werden kann, in wie weit der Mangel einer Erklärung gegenüber der Federal Trade Commission sich auf die Durchsetzbarkeit auswirkt.[61] Darüber hinaus sind ohnehin bezüglich der Rechtsfestigkeit der Privacy-Shield-Entscheidung auch vom EU-Parlament Zweifel artikuliert worden, die nicht zuletzt auch auf den Punkt abzielen, dass Betroffenen keine den EU-Normen vergleichbaren Rechtsschutzmöglichkeiten zur Verfügung stehen.[62]

Insbesondere in dem Fall, in dem ein Arbeitnehmer einer deutschen Universität, sich durch seinen Arbeitgeber veranlasst sieht, an ORCID teilzunehmen, hat – im Konfliktfall – einen deutlich aufwändigeren und mit hoher Wahrscheinlichkeit weniger effektiven Rechtsweg zu beschreiten, als wenn die Verarbeitung innerhalb der EU stattfände, so dass gewisse Zweifel an der Angemessenheit des Schutzniveaus bestehen. Allerdings ist auch eine innereuropäische Rechtsdurchsetzung von Datenschutzrechten keineswegs trivial, so dass hier keine abschließende Einschätzung der unterschiedlichen (tatsächlichen) Schutzniveaus erfolgen kann. Für die Einrichtung, die ORCID mit der Verwaltung ihrer Mitarbeiterdaten betraut, verbleibt soweit ein gewisses Risiko, dass diese Datenverarbeitung als unzulässig angesehen wird. Allerdings ist insofern

---

[58] Punkt 12.0 der Privacy Policy.

[59] Federal Trade Commission (Hrsg.) https://www.privacyshield.gov/list (7.5.2017).

[60] Punkt 12.0 und 13.0 Privacy Policy,

[61] Etwa nach dem Federal Trade Commission Act, der offenkundig in Fällen des Verstoßes gegen die Aussagen der Selbstzertifizierung die Federal Trade Commission zur Verhängung von Sanktionen berechtigt, vgl. https://www.export.gov/article?id=Enforcement-of-Privacy-Shield (7.5.2017).

[62] Europäisches Parlament, „Adequacy of the protection afforded by the EU-US privacy Shield European Parliament resolution of 6 April 2017 on the adequacy of the protection afforded by the EU-US Privacy Shield (2016/3018(RSP))", dort Nr. 6, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2017-0131+0+DOC+PDF+V0//EN (7.5.2017) unter Verweis auf ähnliche Zweifel seitens der Europäischen Datenschutzaufsichtsbehörden (Artikel 29-Gruppe) in lit H.

hervorzuheben, dass sofern nur ohnehin öffentlich verfügbare Informationen eingestellt werden, das Risiko für den Betroffenen und dementsprechend die Schadenspotentiale eher gering ausfallen dürften.

Zusammenfassend ist damit zu empfehlen, dass Einrichtungen, die möchten dass ihre Mitarbeiterinnen und Mitarbeiter eine ORCID iD anlegen eine entsprechende Auftragsdatenvereinbarung mit ORCID abschließen. ORCID ist zu empfehlen hierfür einen Standardtext vorzusehen und die technisch-organisatorischen Maßnahmen extern auditieren lassen. Schließlich wäre erneut zu prüfen, ob es für ORCID nicht doch möglich ist, auch als Non-Profit eine entsprechende Privacy-Shield-konforme Selbstverpflichtung gegenüber dem zuständigen „Department of Commerce" abgeben kann, und so von der Vermutung eines adäquaten Schutzniveaus auf Grundlage der entsprechenden Kommissionsentscheidung (s.o.) profitieren kann. Darüber hinaus ist zu empfehlen, dass die betroffenen Organisationen die weitere Diskussion und Rechtsprechung genau verfolgen und ihre Praxis gegebenenfalls anpassen. Aufgrund der Komplexität des Datenschutzrechts und der geringen Durchdringung durch Rechtsprechung ist darauf hinzuweisen, dass ein rechtliches Risiko selbst unter Berücksichtigung aller Empfehlungen nicht gänzlich ausgeschlossen werden kann.

e) Rechtsgrundlage und Widerspruchsmöglichkeit für Speicherung der E-Mail-Adresse für die Zeit nach Löschung des Profils

ORCID bietet standardmäßig keine Möglichkeit, die Speicherung der E-Mail-Adresse zu widerrufen. Ausweislich der Nutzungsbedingungen kann ein Profil lediglich deaktiviert werden, wobei die E-Mail-Adresse weiter gespeichert wird, um zu vermeiden, dass derselbe Identifikator (die ORCID iD) einer anderen Person zugewiesen wird, und um Nutzerinnen und Nutzern zu ermöglichen, den Identifikator wieder aktivieren zu können.[63]

Eine solche Speicherung könnte auf die gesetzliche Rechtsgrundlage des § 28 Abs. 1 Satz 1 oder Satz 2 BDSG zu stützen sein.[64] Hiernach ist eine Speicherung dann zulässig, wenn entweder - nach Satz 1 - die Daten für die Durchführung eines rechtsgeschäftsähnlichen Schuldverhältnisses oder - nach Satz 2 – zur

[63] Orcid.org, „Privacy Policy", unter Nr. 8: „You may choose to disable your ORCID Record in the Registry by deactivating the Account from the Account Settings page of your Record. In the event that an ORCID Record is disabled, we will maintain as Private your email address, so as not to assign the same identifier to another person and to allow you to re-claim your identifier in the future.", online: https://orcid.org/footer/privacy-policy (23.3.2017).

[64] Die entsprechenden Vorschriften des eigentlich anwendbaren TMG sind seit EuGH C-582/14 (Breyer gg. Deutschland), Rn. 50 bis 64, gesperrt bzw. entsprechend auszulegen.

Wahrung berechtigter Interessen der Verantwortlichen Stelle erforderlich ist (und im letzteren Fall: „kein Grund zur Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung überwiegt"). Sofern man das Verhältnis zwischen ORCID und den Nutzerinnen und Nutzern als ein rechtsgeschäftsähnliches Schuldverhältnis qualifizieren möchte, wäre damit die Speicherung zulässig; jedenfalls aber bei Nichtvorliegen eines solchen, zur Wahrung der berechtigten Interessen, weil die Speicherung ja dem Zweck dient Verwechselungen zu vermeiden, was im Zentrum des Angebots und Ziels von ORCID steht.

Darüber hinaus hat ORCID auf Nachfrage dargestellt, dass sie auf Anforderung die E-Mail-Adresse löschen, so dass eine Widerruflichkeit der Speicherung gegeben ist. Insofern ist zu empfehlen, auf diese Möglichkeit in der Privacy Policy ausdrücklich hinzuweisen.

f) Zwischenfazit

Eine Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten ist grundsätzlich gegeben. Die Verarbeitung der Registrierungs-, Profil- und Nutzungsdaten durch ORCID Inc. kann auf eine wirksame Einwilligungserklärung gestützt werden. In Hinsicht auf die Profildaten stellt die Privacy-Funktionalität mit ihren weitergehenden Transparenz- und Kontrollmöglichkeiten eine vorbildliche Umsetzung dar. Die fortdauernde Speicherung der E-Mail-Adresse kann gegebenenfalls auf den gesetzlichen Erlaubnistatbestand der „berechtigten Interessen" gestützt werden. Sie ist außerdem widerruflich gestaltet, worauf allerdings in der Privacy Policy hinzuweisen ist.

4. Prinzipien der Zweckbindung und Erforderlichkeit

Die Verarbeitung der personenbezogenen Daten unterliegt neben der Erfordernis einer Rechtsgrundlage zusätzlichen Grundsätzen, von denen hier die Prinzipien der Zweckbindung und der Erforderlichkeit hervorgehoben werden sollen. Diese Prinzipien besagen, dass der Verarbeiter vor Erhebung der personenbezogenen Daten die Zwecke der Verarbeitung hinreichend präzise bestimmen muss. Die Daten dürfen sodann grundsätzlich nur für die Zwecke verarbeitet werden, die der Verarbeiter ursprünglich angegeben hat. Die Daten dürfen außerdem nur erhoben und verarbeitet werden, soweit sie für diese Zwecke jeweils erforderlich sind. Das Zweckbindungsprinzip soll für die Betroffenen sicherstellen, dass Transparenz und Kontrollierbarkeit der Datenverarbeitung gewährleistet sind.[65]

[65] Art. 29 Datenschutzgruppe, „Opinion 03/2013 on purpose limitation", S. 13 und 14.

Inwieweit die in der Privacy Policy angegebenen Zwecke hinreichend präzise bestimmt sind bzw. ob die Verarbeitung der jeweiligen Daten für diese Zwecke erforderlich ist, wird im nachfolgenden Teil V untersucht. Im Übrigen wird hier unterstellt, dass die tatsächliche Verarbeitung der Daten durch die Plattform den Zwecken entspricht, die in der Privacy Policy angegebenen werden. Insofern ist die Erhebung und Verarbeitung der Daten für die angegebenen Zwecke zumindest grundsätzlich erforderlich (siehe ebenfalls sogleich in Bezug auf die jeweiligen Datenkategorien).

Konflikte mit den vorgenannten Prinzipien können allerdings durch spätere Datenverarbeitungen auftreten, sofern diese für andere Zwecke als die ursprünglich in der Privacy Policy angegeben Zwecke erfolgen. Dafür muss entweder eine erneute Einwilligung der Nutzerinnen und Nutzer vorliegen oder sie müssen sich auf eine andere Rechtsgrundlage stützen (siehe Teil V.).

5. Flankierend: Transparenz, Sicherheit und Kontrolle

Flankierend zu den vorgenannten Prinzipien trifft das Datenschutzrecht zahlreiche Regelungen, die insbesondere die Bereiche Transparenz, IT-Sicherheit und Kontrolle berühren.

a) Transparenz

Transparenzerfordernisse ergeben sich vorliegend insbesondere aus § 13 Abs. 1 TMG, wonach der Diensteanbieter „den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten sowie über die Verarbeitung seiner Daten in Staaten außerhalb des Anwendungsbereichs der 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 (ABl. EG Nr. L 281 S. 31) in allgemein verständlicher Form zu unterrichten" hat. Außerdem muss der "[d]er Inhalt der Unterrichtung [...] für den Nutzer jederzeit abrufbar sein."

Diesen Anforderungen wird der Betreiber ORCID durch die in der Fußzeile jeder Webseite verlinkte Privacy Policy grundsätzlich gerecht (zur hinreichenden Bestimmtheit der Zweckangaben sei wieder auf den nachfolgenden Teil 5 verwiesen). Dabei ist anerkannt, dass ein solcher direkter, mit „Datenschutz" oder „Privacy" gekennzeichneter Link auf eine entsprechende Darstellung für eine

Unterrichtung zu Beginn des Nutzungsvorganges ausreichend sein soll.[66] Sofern die vorgenannte Privacy Policy die tatsächlichen Nutzungen erfasst – was in diesem Rahmen ohne Auditierung[67] des technischen Systems nicht überprüft werden kann, ist damit also der Anforderung des § 13 Abs. 1 TMG genüge getan. Allerdings könnte man bezweifeln, dass die für eine Datenerhebung in Deutschland erforderliche „allgemein verständliche Form" mit einer englischsprachigen Erklärung erreicht werden kann.[68]

Ebenfalls durch die Privacy Policy abgedeckt werden die Pflichten aus § 13 Abs. 2 TMG, wonach eine Pflicht zur Unterrichtung besteht, sofern Cookies zur Re-Identifizierung von Nutzenden eingesetzt werden (Ziff. 5.0 der Privacy Policy).

Der Pflicht zum Hinweis auf das bestehende Widerrufsrecht bei Einwilligungen zur Datenverarbeitung von personenbezogenen Daten wird durch den Hinweis auf die Möglichkeit der Datenlöschung in Ziff. 8 der Privacy Policy nachgekommen.

Sofern auch Profilbildungen durchgeführt werden, besteht diesbezüglich eine Hinweispflicht nach § 15 Abs. 3 TMG. Im Kern des Dienstes stehen neben der Vergabe der ORCID iD vor allen Dingen auch die Pflege eines eigenen Profils, das völlig unter der Kontrolle der Betroffenen steht. Es ist für die Nutzer damit offensichtlich, dass insoweit ein Profil entsteht. Eine darüberhinausgehende Hinweispflicht würde nur bestehen, sofern weitere, für die Nutzer verborgene Profile im System erstellt würden. Eine Erstellung solcher Profile erfolgt nach Angaben des Auftraggebers derzeit nicht.

Gemäß § 13 Abs. 2 Nrn. 3 und 4 TMG muss der Nutzende den Einwilligungsinhalt jederzeit abrufen und der Verarbeitung widersprechen können. Dieser Anforderung trägt ORCID in Hinblick auf die Profildaten durch die feingranula-

---

[66] Spindler/Schuster, Recht der elektronischen Medien, 3. Auflage 2015, § 13 Rn 8.

[67] Die Plattform ORCID weist ein Datenschutz-Gütesiegel der Firma TRUSTe auf. Hierdurch wird deutlich, dass sich die Betreiber (privatrechtlich gegenüber TRUSTe) zur Einhaltung der Anforderungen der „Enterprise Certification Standards" verpflichtet haben. Allerdings kommt dies einer Auditierung nicht gleich. Zwar müssen die Betreiber TRUSTe zum Führen dieses Siegels Einsichtsrechte in die Datenverarbeitung gewähren, aber die Einhaltung der Angaben des verpflichteten Betreibers werden dabei ebenso wenig geprüft, wie die Einhaltung deutschen oder europäischen Rechts, vgl. TRUSTe Certification, https://orcid.org/content/orcid-privacy-policy#TRUSTe, unter Verweis auf https://privacy.truste.com/privacy-seal/validation?rid=0457b0e6-f622-42b6-b7f8-9258324d813a, wo es heisst: „Das Unternehmen ist für die interne Kontrolle und die Wirksamkeit seiner Datenschutzrichtlinien, Erklärungen, Prozesse und Verfahren verantwortlich. TRUSTe verlässt sich bei der Ermittlung, ob das Unternehmen die Zertif-ikatstandards von TRUSTe erfüllt, auf die Genauigkeit der vom Unternehmen angegebenen Informationen sowie auf andere Nachweise."

[68] In diese Richtung weist etwa das Urteil des LG Berlin vom 9. Mai 2014, (15 O 44/13), online: http://www.vzbv.de/cps/rde/xbcr/vzbv/WhatsApp-LG-Berlin-15_0_44_13.pdf, allerdings in Bezug auf die Impressumspflicht und Allgemeine Geschäftsbedingungen.

ren Einstellungen für die einzelnen Datenbestände Rechnung, zudem können die Nutzerinnen und Nutzer ihr Profil vollständig löschen.[69]

Schließlich besteht nach § 13 Abs. 8 TMG die Pflicht zur Auskunfterteilung bei Anfragen zur Person. Hierdurch wird schon durch die Angaben im persönlichen Profil gedient. Für darüber hinaus gehende Anfragen nennt die Privacy Policy einen Ansprechpartner mit Post- und E-Mailanschrift.

Die Transparenzanforderungen des TMG sind bei ORCID eingehalten, allerdings ist zu empfehlen auch eine deutsche Fassung der Privacy Policy vorzusehen.

b) Sicherheit

Anforderungen an die technische Sicherheit einer Plattform ergeben sich insbesondere aus § 9 BDSG (nebst Anlage), wonach angemessen technische und organisatorische Maßnahmen zu ergreifen sind, die sicherstellen, dass die datenschutzrechtlichen Vorschriften eingehalten werden. Ähnliche Anforderungen ergeben sich aus Art. 32 DSGVO, wobei hiernach nicht nur der Verantwortliche, sondern ausdrücklich auch der Auftragsdatenverarbeiter für die Umsetzung der Datensicherheitsmaßnahmen verantwortlich ist. Ob diese Vorgabe eingehalten wird, lässt sich im Rahmen dieser Untersuchung nicht abschließend beurteilen. Hierfür wäre eine Auditierung erforderlich.

c) Kontrolle

Um die Einhaltung der datenschutzrechtlichen Vorschriften zu unterstützen, ist bei nicht-öffentlichen Stellen unter bestimmten Voraussetzungen eine Datenschutzbeauftragte oder ein Datenschutzbeauftragter zu bestellen (in der Regel ab 10 Personen, die mit der Datenverarbeitung beschäftigt sind, § 4 lit. F Abs. 1 S. 3 BDSG). Die Anzahl der Mitarbeiter, die bei ORCID auf der Internetseite vorgestellt werden, deutet darauf hin, dass die entsprechenden Schwellwerte noch nicht überschritten sind. Insofern ist darauf hinzuweisen, dass die DSGVO diese Schwellwerte maßgeblich modifiziert. Nach Art. 37 Abs. 1 DSGVO müssen der Verantwortliche (aber auch der Auftragsdatenverarbeiter) nur dann einen Datenschutzbeauftragten bestellen, wenn die verarbeiteten Daten gemäß Art. 9 DSGVO besonders sensibel sind oder die Datenverarbeitung „aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich“ macht.

[69] Bezüglich der Nutzungsdaten s.u. Teil IV. Nr. 1. lit. b) und lit. c), zur E-Mail-Adresse s.o. Nr. 3. lit. e).

Danach wird – auf Grundlage der bisherigen Faktenlage - keine Verpflichtung von ORCID zur Bestellung eines Datenschutzbeauftragten bestehen.

Allerdings erscheint im vorliegenden Fall die Bestellung einer Datenschutzbeauftragten oder eines Datenschutzbeauftragten ratsam, weil im Team von ORCID laut Webseite ohnehin ein „Privacy Specialist" tätig ist.[70] Daher würde es sich anbieten – die erforderliche Sachkunde unterstellt – diesen „Privacy Specialist" schriftlich auch im Sinne des BDSG beziehungsweise der bald[71] in krafttretenden DSGVO als Datenschutzbeauftragten zu bestellen. Dieser könnte dann für datenschutzrechtliche Fragen im laufenden Geschäft als permanenter Ansprechpartner zur Verfügung stehen. Dabei ist zu berücksichtigen, dass nach der vorherrschenden Auslegung des Datenschutzrechts, diese Funktion nicht durch die Geschäftsführung übernommen werden darf, weil sich hier ein Interessenkonflikt ergeben kann. Die Geschäftsführung trifft nach der Konzipierung des Datenschutzrechtes – anders als den Datenschutzbeauftragten – zwar die Verantwortung für die rechtmäßige Verarbeitung, aber (oder besser gerade deswegen) fehlt es regelmäßig an der erforderlichen Unabhängigkeit bei der Beurteilung.

d) Zwischenfazit

Gegenüber den datenschutzrechtlichen Anforderungen in den Bereichen der Transparenz, Sicherheit und Kontrolle sind keine Konflikte erkennbar, allerdings sind kleinere Nachjustierungen zu empfehlen. Die Datenschutzerklärung sollte auch in deutscher Sprache vorgehalten werden. Die technische Sicherheit könnte durch eine externe Auditierung oder Zertifizierung belegt werden und ein Datenschutzbeauftragter, der mit hinreichender Unabhängigkeit ausgestattet ist, sollte bestellt werden.

[70] https://orcid.org/content/orcid-team (23.5.2017).
[71] Vgl. S. 22.

IV. Zweckbindung und Erforderlichkeit einzelner Nutzungsszenarien

Nachdem im vorangegangenen Teil III eine allgemeine Prüfung der datenschutzrechtlichen Voraussetzungen der Datenverarbeitungen vorgenommen wurde, liegt der Schwerpunkt des vorliegenden Teils auf der Prüfung der Rechtmäßigkeit der einzelnen Zweckangaben sowie der Erforderlichkeit der entsprechenden Datenverarbeitungen. Die Prüfung folgt dabei dem Aufbau, der insbesondere unter den Punkten III. 1 und 2 zur Kategorisierung der verarbeiteten personenbezogenen Daten und zur Verantwortlichkeit entwickelt wurde. Danach ergeben sich die folgenden Prüfungsschwerpunkte: erstens die Verarbeitung der jeweiligen personenbezogenen Daten durch ORCID, zweitens die Verarbeitung der personenbezogenen Daten durch „Trusted Organizations" und drittens die Verarbeitung der öffentlich gemachten Daten durch jedermann. Abschließend wird auf die datenschutzrechtlichen Voraussetzungen für eventuelle Zweckänderungen eingegangen.

1. Verarbeitungszwecke von ORCID

Wie in Teil III. unter Nr. 2 lit. a) dargestellt, erhebt und verarbeitet ORCID die personenbezogenen Daten vornehmlich zu den folgenden drei Zwecken: primär, um Wissenschaftlerinnen und Wissenschaftler global eindeutig identifizieren und ihnen Werke eindeutig zuordnen zu können (im Folgenden auch „Zwecke des Identitätsmanagements"); um die eigenen Webseiten instand zu halten, zu evaluieren und verbessern zu können; und um die Nutzerinnen und Nutzer des Portals für bestimmte Zwecke kontaktieren zu können.

a) Verarbeitung von Registrierungs- und Profildaten für Zwecke des Identitätsmanagements

ORCID Inc. verarbeitet die personenbezogenen Daten der Nutzerinnen und Nutzer der Plattform für den Zweck, Wissenschaftlerinnen und Wissenschaftler global eindeutig identifizieren und ihnen Werke eindeutig zuordnen zu können. Dazu gehört die Lösung potentieller Identifizierungs- und Zuordnungskonflikte. Fraglich ist, inwieweit diese Zweckbestimmung hinreichend präzise ist beziehungsweise inwieweit die Erhebung und Verarbeitung der personenbezogenen Daten für diesen Zweck erforderlich ist.

Dieser Zweck wird in der Privacy Policy nicht ausdrücklich weiter definiert. Allerdings lässt sich aus dem Kontext, das heißt, den sonstigen Angaben der Privacy Policy sowie aus der Funktionalität der Plattform auf bestimmte Unterfälle

schließen.[72] So können Konflikte insbesondere in den folgenden drei Fällen auftreten: erstens, wenn bei einer Neuregistrierung eine E-Mail-Adresse verwendet wird, die bereits einem anderen Profil zugeordnet ist; zweitens, wenn unterschiedliche Nutzerinnen oder Nutzer des Portals oder noch nicht registrierte Wissenschaftlerinnen oder Wissenschaftler die Urheberschaft für das selbe registrierte Werk beanspruchen; oder drittens, wenn einer Nutzerin oder einem Nutzer des Portals von Dritten Angaben zugeschrieben werden, mit denen er oder sie nicht einverstanden ist.

Damit lässt sich der angegebene Zweck (auch durch die Nutzerinnen und Nutzer der Plattform) hinreichend bestimmen. Darauf aufbauend ist es möglich zu untersuchen, ob die Erhebung und Verarbeitung der einzelnen Daten für diesen Zweck erforderlich ist. Für die eindeutige Identifizierung von Wissenschaftlerinnen und Wissenschaftlern ist die Erhebung der Registrierungsdaten, hier einer E-Mail-Adresse und eines Vornamens (eine Klarnamenpflicht ist nicht vorgesehen), erforderlich, um den Nutzer zu authentifizieren (die Erhebung des Passworts ist zudem erforderlich, um den autorisierten Zugang zu dem Profil abzusichern). Für die Konfliktlösung ist die Weitergabe der hinterlegten E-Mail-Adresse der Konfliktparteien erforderlich.

Fraglich ist allerdings, ob die Speicherung der E-Mail-Adresse auch dann erforderlich ist, wenn eine Nutzerin oder ein Nutzer ihr oder sein Profil auf der Plattform löscht.[73] Gegen eine Erforderlichkeit könnte sprechen, dass mit Löschung des Profils auch die E-Mail-Adresse nicht mehr benötigt wird. Insofern ist jedoch darauf hinzuweisen, dass die E-Mail-Adresse durch ORCID nur deshalb standardmäßig auch für die Zeit nach Löschung des Profils gespeichert wird, um der Nutzerin oder dem Nutzer die Möglichkeit zu geben, später – im Falle einer Meinungsänderung – das Profil wiederaufleben zu lassen und dabei die unter der E-Mail-Adresse angelegte ORCID iD wiederverwenden zu können. Da die standardmäßige Speicherung der E-Mail-Adresse also zu dem Zweck erfolgt, eine lebenslange Zuordnung von Werken zu ermöglichen, kann die standardmäßige Speicherung der E-Mail-Adresse für die Zeit nach Löschung des Profils als erforderlich angesehen werden. Dabei ist darauf hinzuweisen, dass die Nutzerin oder der Nutzer der Speicherung ihrer oder seiner E-Mail-Adresse für die Zeit nach Löschung des Profils jederzeit widersprechen kann.[74]

Die Erstellung und Bearbeitung von in einem ORCID-Profil gespeicherten Profilangaben ist ebenfalls für die Identifizierung der Wissenschaftlerin oder des

---

[72] Vgl. zur Auslegung der Zweckangabe entsprechend dem Kontext bei Art. 29 Datenschutzgruppe, Opinion 03/2013 on purpose limitation, S. 16.
[73] Siehe hierzu bereits unter Punkt III. 3. e) „Exkurse: Erlaubnisvorschrift für Speicherung der E-Mail-Adresse".
[74] Siehe oben unter Punkt III. 1. e) „Gesetzliche Grundlage

Wissenschaftlers zumindest insoweit erforderlich, als die Wissenschaftlerin oder der Wissenschaftler diese Angaben bewusst über die Privacy-Funktionalität für diese Zwecke freigibt.

Fraglich ist jedoch, ob die Verarbeitung solcher Daten für die Konfliktlösung erforderlich ist, die Nutzende als „private" oder „limited access" markiert hat. ORCIDs Privacy Policy gibt insofern an: „we may use such data for disambiguation or to resolve any disputes about identity and Records".[75] Zumindest wenn Angaben „private" sind, wird es kaum zu Konflikten kommen, da kein Dritter die Angaben sehen kann. Anders verhält es sich mit Angaben, die unter „limited access" stehen, weil diese zumindest von bestimmten Dritten eingesehen werden können. Die Verarbeitung von als „private" markierten Daten ist nur erlaubt, wenn dies im Einzelfall für die Lösung von Konflikten unbedingt erforderlich ist, was nach Angaben des Betreibers auch ihrer internen Praxis entspricht.

b) Verarbeitung der Nutzungsdaten für Zwecke des Identitätsmanagements

Fraglich ist, ob die Erhebung und Verarbeitung von Nutzungsdaten (also der Daten, die bei der Nutzung der Webseite anfallen, wie Verweildauer, IP-Adresse und ähnliches) erforderlich ist, um eine Identifizierung der Wissenschaftlerinnen oder Wissenschaftler, eine Zuordnung ihrer Werke sowie die Lösung entsprechender Konflikte zu ermöglichen. Eine solche Erforderlichkeit kann sich insofern ergeben, um zu überprüfen, wer wann welche Angaben auf dem Portal vorgenommen hat, zum Beispiel, ob eine Angabe von der Nutzerin oder dem Nutzer selbst oder einer „Trusted Party" gemacht wurde. Weitere Nutzungsdaten wären hierfür dagegen nicht erforderlich. Insofern Nutzungsdaten nicht für Zwecke des Identitätsmanagements verwendet werden, sollte eine Klarstellung in der Privacy Policy erfolgen.

c) Verarbeitung der Nutzungsdaten für die Instandhaltung, Evaluierung und Verbesserung der Plattform

ORCID Inc. verarbeitet die personenbezogenen Daten der Nutzerinnen und Nutzer der Plattform ebenfalls dafür, um die technische Infrastruktur der Plattform instand zu halten, zu evaluieren und zu verbessern. Die Artikel-29-Datenschutzgruppe, das unabhängige Beratungsgremium der Europäischen Kommission in Fragen des Datenschutzes, ist diesbezüglich der Meinung, dass die Zweckangaben „improving user experience" und „IT security" nicht hinrei-

[75] Punkt 6.0 Privacy Policy.

chend präzise sind.[76] Danach wäre die Angabe in ORCIDs Privacy Policy, dass die Daten für das Instandhalten der Webseiten, ihre Evaluierung sowie Verbesserung verwendet werden, nicht hinreichend bestimmt.

Der Europäische Gerichtshof hat jüngst entschieden, dass der Betreiber einer Webseite (als der datenschutzrechtlich Verantwortliche) „*may also have a legitimate interest in ensuring, in addition to the specific use of their publicly accessible websites, the continued functioning of those websites*."[77] Der EuGH definiert also den Zweck, personenbezogene Daten zu erheben und zu speichern, um eine Webseite generell instand zu halten, als legitim im Sinne des Art. 7 lit. f RL 95/46/EC. Damit lässt sich nur mehr schwer argumentieren, dass zumindest dieser Zweck trotz seiner grundsätzlichen Legitimität nicht hinreichend bestimmt sein soll.

Es ist jedoch darauf hinzuweisen, dass sich die Entscheidung des EuGH auf einen sehr eingeschränkten Datenbestand bezog, vor allem auf die IP-Adresse des Betroffenen, unter der dieser zu einem bestimmten Zeitpunkt auf die Webseite zugreift.[78] Daher ist ORCID zu empfehlen, die Erforderlichkeit der jeweils erhobenen und verarbeiteten personenbezogenen Datenkategorien für die Zwecke der Instandhaltung, Evaluierung und Verbesserung der Plattform genau zu prüfen. Um das rechtliche Risiko einer „nicht-erforderlichen" Verarbeitung zu reduzieren, kann es zudem ratsam sein, die Daten für diese Zwecke so weit wie zweckverträglich zu anonymisieren. In der Privacy Policy sollte dementsprechend klargestellt werden, dass die Nutzungsdaten darüber hinaus nicht verwendet werden.

d) Verarbeitung der Registrierungsdaten für Kontaktierungszwecke

Hinreichend bestimmt sind die in der Privacy Policy angegebenen Zwecke, für die ORCID Inc. den Nutzenden kontaktiert: erstens, um Anfragen einer Mitgliedsorganisation von ORCID, die Wissenschaftlerin oder den Wissenschaftler als „Trusted Party" zu kennzeichnen, an sie oder ihn weiterzureichen. Zweitens, um die Nutzerinnen und Nutzer über Änderungen der Datenschutzerklärung oder Nutzungsvereinbarung von ORCID, zum Beispiel über Änderungen des Registrierungsprozesses, der Privacy-Funktionalität oder der jeweils erhobenen Daten zu informieren. Allerdings wird für eine Zweckänderung bezüglich bereits erhobener personenbezogener Daten auf die schon dargelegte Darstellung (Teil III. 4.) verwiesen, dass eine solche Änderung gegebenenfalls auf eine neue Einwilligung oder eine andere legitime Rechtsgrundlage gestützt werden

[76] Artikel-29-Datenschutzgruppe, Opinion 03/2013 on purpose limitation, S. 16.
[77] EuGH C-582/14 (Breyer gg. Deutschland), Rn. 60.
[78] EuGH C-582/14 (Breyer gg. Deutschland), Rn. 14.

muss (siehe zu den allgemeinen Voraussetzungen den folgenden Abschnitt 3.). Drittens, um Nutzerinnen und Nutzern einen Newsletter mit Informationen über ORCID zuzusenden, wobei sie die Möglichkeit zum Opt-out erhalten. Die Nutzerin oder der Nutzer der Plattform kann hier die Zwecke der Verwendung der Daten hinreichend genau erkennen. Die rechtlich korrekte Umsetzung des Opt-out-Mechanismus wird hier vorausgesetzt.

e) Zwischenfazit

Die Zwecke der Verarbeitung von Registrierungs- und Profildaten für das Identitätsmanagement durch ORCID lässt sich anhand des Kontextes (auch durch die Nutzerinnen und Nutzer des Portals) hinreichend bestimmen. Die Verarbeitung der Registrierungsdaten für diese Zwecke ist erforderlich. Auch die standardmäßige Speicherung der E-Mail-Adresse für die Zeit nach Löschung des Profils wird hier als erforderlich betrachtet, soweit dies der Nutzerin oder dem Nutzer die Möglichkeit erhalten soll, ihr oder sein Profil zu einem späteren Zeitpunkt wieder aufleben zu lassen (die Nutzerinnen und Nutzer des Portals können zudem der fortdauernden Speicherung zu jedem Zeitpunkt widersprechen). Auch die Verarbeitung der Profilangaben ist für die Identitätsmanagementzwecke erforderlich. Allerdings ist die Erforderlichkeit für als „private" markierte Daten für diese Zwecke im Einzelfall genau zu prüfen. Sofern Nutzungsdaten nicht für Zwecke des Identitätsmanagements verwendet werden, sollte eine Klarstellung in der Privacy Policy erfolgen.

Die Erforderlichkeit der Verarbeitung von Nutzungsdaten für Zwecke der Instandhaltung, Evaluierung und Verbesserung der Plattform hängt maßgeblich von der eingesetzten Anonymisierungstechnik ab. Diese ist im Einzelfall genau zu prüfen. In der Privacy Policy sollte klargestellt werden, dass die Nutzungsdaten darüber hinaus nicht verwendet werden.

Schließlich erfolgt die Verarbeitung der Registrierungsdaten zur Kontaktaufnahme für hinreichend bestimmte Zwecke. Insofern ist die Verarbeitung auch erforderlich.

2. Verarbeitung durch Dritte zu eigenen Zwecken

Die personenbezogenen Daten werden zudem von Dritten für eigens gesetzte Zwecke verarbeitet. Dies sind vorliegend die „Trusted Organizations" sowie alle sonstigen Dritten, die auf die veröffentlichten Daten zugreifen können und für jeweils eigene Zwecke verarbeiten können.

a) Keine Verantwortlichkeit von ORCID (Maßnahmen von ORCID, die über gesetzliche Anforderungen hinausgehen)

Da hier wie oben dargestellt angenommen wird, dass die „Trusted Individuals" ausschließlich Zwecke mit Mitteln verfolgen, die ihnen von der Nutzerin oder dem Nutzer des Portals vorgegeben werden, verbleibt die Verantwortlichkeit für die daraus resultierenden Risiken allein bei letzteren.[79] Insofern findet keine gesonderte beziehungsweise erneute Prüfung der Zwecke statt.

Anders als „Trusted Individuals" verarbeiten „Trusted Organizations" sowie sonstige Dritte die personenbezogenen Daten zumindest auch für ihre eigenen Zwecke. Soweit sie die Daten ausschließlich für diese eigenen Zwecke verarbeiten, sind sie datenschutzrechtlich „verantwortliche Stelle". Wie dargestellt trifft ORCID für diese selbstgesetzten Zwecke Dritter keine eigene Verantwortlichkeit. [80]

Trotzdem stellt ORCID den Nutzerinnen und Nutzern des Portals über die Privacy-Funktionalität wichtige Kontrollmöglichkeiten zur Verfügung. Zwar ist keine Kontrolle möglich, zu welchen Zwecken öffentliche Profildaten durch Dritte verwendet werden. Die Nutzerin oder der Nutzer des Portals können aber kontrollieren, ob Dritte überhaupt Zugriff auf die jeweiligen Profilangaben bekommen. Darüber hinaus sieht ORCID weitere Maßnahmen zum Schutz der Profilinhaber vor. Insbesondere verpflichtet ORCID „Trusted Organizations" in seiner Kooperationsvereinbarung, für bestimmte Zwecke weitere Einschränkungen einzuhalten. Dies betrifft die Weitergabe von Profildaten an Dritte sowie die Nutzung der Angaben für Marketing.

b) Verarbeitung der „limited access"-Daten durch „Trusted Organizations" (insbesondere zur Weitergabe an Dritte und zu Marketingzwecken)

Laut Privacy Policy stellt ORCID über Vereinbarungen mit den „Trusted Organizations" sicher, dass diese personenbezogene Daten, die die Nutzerinnen und Nutzer des Portals unter „limited access" zur Verfügung stellen, grundsätzlich nicht an Dritte weitergeben dürfen. Eine solche Weitergabe ist nur erlaubt, wenn sie die Nutzerin oder den Nutzer darüber informieren, an wen und wie sie die Daten weitergeben möchten. Entsprechendes gilt für Marketingzwecke, die „Trusted Organizations" mit der Verarbeitung der personenbezogenen Daten verfolgen könnten. Über eine Vereinbarung stellt ORCID sicher, dass „Trus-

[79] Siehe hierzu bereits oben unter Punkt IV. 2. „Regelungsadressat: Verantwortliche Stelle".
[80] Siehe hierzu bereits oben unter Punkt IV. 2. „Regelungsadressat: Verantwortliche Stelle".

ted Organisations“ einen Opt-out-Mechanismus für die Nutzerinnen und Nutzers des Portals anbieten müssen, wenn sie die Daten für Marketingzwecke verwenden möchten. Da ORCID selbst keine Verantwortlichkeit für diese Verarbeitungszwecke trifft, geht ORCID hier über seine eigene gesetzliche Verpflichtung hinaus.[81]

c) Verarbeitung der „public“ Daten durch jedermann

Sonstige Dritte können nur die Daten einsehen, die die Nutzerin oder der Nutzer des Portals veröffentlicht hat. Insofern findet durch ORCID ausdrücklich keine Zweckbegrenzung statt. Da die Erstveröffentlichung durch ORCID auf der ausdrücklichen Einwilligung der Nutzerin oder des Nutzers beruht, liegt die datenschutzrechtliche Verantwortlichkeit zunächst bei der Nutzerin oder dem Nutzer sowie grundsätzlich bei dem Dritten, der die veröffentlichten Daten für eigene Zwecke weiterverarbeitet.[82] Da diese Zwecke mangels Anhaltspunkten nicht vorhergesehen werden können, sind sie einer rechtlichen Prüfung in diesem Gutachten kaum zugänglich. Allerdings können die Grundzüge einer solchen Prüfung dargestellt werden (siehe im nun folgenden Abschnitt).

d) Zwischenfazit

ORCID trifft keine Verantwortlichkeit, soweit personenbezogene Daten ausschließlich gemäß Zwecksetzung Dritter verarbeitet werden. So trägt eine Nutzerin oder ein Nutzer des Portals die Verantwortlichkeit selbst, soweit „Trusted Individuals“ ausschließlich Zwecke mit Mitteln verfolgen, die ihnen von der Nutzerin oder dem Nutzer vorgegeben werden. Anders als „Trusted Individuals“ verarbeiten „Trusted Organizations“ sowie sonstige Dritte die personenbezogenen Daten zumindest auch für ihre eigenen Zwecke. Soweit die Daten ausschließlich für diese eigenen Zwecke verarbeiten, sind sie datenschutzrechtlich „verantwortliche Stelle“.

3. Neue Verarbeitungszwecke

Die Verarbeitung personenbezogener Daten zu neuen Zwecken, das heißt, zu anderen Zwecken als bei ihrer Erhebung angegeben, bedarf einer neuen Rechtmäßigkeitsprüfung. Das Zweckbindungsprinzip verbietet die Weiterverarbeitung personenbezogener Daten für andere Zwecke nicht per se. Stattdes-

---

[81] Vgl. bereits die Privacy-Funktionalität als Plus zur herkömmlichen Einwilligung des Nutzers oben unter Punkt III. 3 c) „Weitere Transparenz- und Kontrollmechanismen durch die Privacy-Funktionalität“.

[82] Siehe bereits oben unter Punkt III. 2. a) „Verantwortlichkeit weiterer Nutzer der Daten“; siehe aber EuGH C-131/12 (González gg. Google Spanien) zum Fall einer rechtswidrigen Weiterverarbeitung von ursprünglich rechtmäßig erhobenen und veröffentlichten Daten.

sen bedarf es entweder einer Verhältnismäßigkeitsprüfung (im deutschen Recht) oder einer Zweckvereinbarkeitsprüfung (im europäischen Recht).

a) Deutsche Rechtslage

Im deutschen Recht ist die Zweckänderung grundsätzlich erlaubt, „soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt" (§ 28 Abs. 2 Nr. 1 i.V.m. Abs. 1 S. 1 Nr. 2 BDSG). Die Verarbeitung veröffentlichter Daten für andere Zwecke erhält demgegenüber eine Privilegierung. Sie ist erst dann ausgeschlossen, wenn das Interesse der Nutzerin oder des Nutzers an dem Ausschluss der Weiterverarbeitung offensichtlich überwiegt (§ 28 Abs. 2 Nr. 1 i.V.m. Abs. 1 S. 1 Nr. 3 BDSG).

Im Forschungskontext gibt es außerdem eine Sondervorschrift (§ 28 Abs. 2 Nr. 3 BDSG), nach der eine Zweckänderung nur dann zulässig ist, wenn

- „es im Interesse einer Forschungseinrichtung zur Durchführung wissenschaftlicher Forschung erforderlich ist,
- das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt
- und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann."

Von einem unverhältnismäßigen Mehraufwand wird ausgegangen, wenn er mehr als 10 Prozent der Gesamtkosten beträgt.[83] Neben dieser Regelung der Voraussetzungen der Datenverarbeitung für neue Forschungszwecke regelt § 40 BDSG, wie die Verarbeitung durchzuführen ist. Nach Abs. 2 sind die Daten – soweit es der Zweck zulässt – zu anonymisieren oder wenigstens zu pseudonymisieren. Nach Abs. 1 gilt außerdem eine strikte Zweckbindung: Wenn die Daten einmal für wissenschaftliche Zwecke erhoben oder gespeichert wurden, dürfen sie für keinen anderen Zweck mehr verwendet werden.

b) Europäische Rechtslage

Im europäischen Recht ist eine Zweckänderung rechtmäßig, wenn der neue Zweck nicht unvereinbar mit dem ursprünglichen Zweck ist, Art. 6 Abs. 1 lit. b RL 95/46/EG. Dasselbe gilt gemäß Art. 5 Abs. 1 lit. b DSGVO, wobei Art. 6 Abs. 4

[83] Plath, Plath, BDSG/DSGVO, § 28 BDSG, Rn. 98.

DSGVO klarstellt, nach welchen Kriterien eine solche Zweckvereinbarkeitsprüfung vorzunehmen ist. Danach ist auf die Verbindung zwischen den unterschiedlichen Zwecken abzustellen; auf den Zusammenhang, in dem die Daten erhoben wurden; die Art der personenbezogenen Daten; die möglichen Folgen für den Betroffenen sowie das Vorhandensein geeigneter Schutzmaßnahmen, wie zum Beispiel Verschlüsselung oder Pseudonymisierung der Daten.

Für die Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken sieht Art. 89 DSGVO eine sogenannte Öffnungsklausel vor. Danach können die Mitgliedsstaaten vorbehaltlich bestimmter Garantien Ausnahmen von bestimmten Rechten und Garantien vorsehen. Wie oben bereits angesprochen liegt insofern bisher lediglich ein Referentenentwurf vor.

c) Zwischenfazit

Die Rechtmäßigkeit neuer (in diesem Gutachten nicht untersuchter) Zwecke kann mangels weiterer Anhaltspunkte nur entlang der grundsätzlichen rechtlichen Leitlinien dargestellt werden. Im Detail muss die Prüfung der Rechtmäßigkeiten daher jeweils anhand des konkreten Einzelfalls erfolgen.

V. Fazit und Empfehlungen

Die datenschutzrechtliche Begutachtung von ORCID hat keine gravierenden Mängel feststellen können. Im Gegenteil, das System unterstützt mit seinen Privacy-Funktionalitäten die Nutzerinnen und Nutzer bei der Ausübung ihres Rechts auf informationelle Selbstbestimmung und hat diesbezüglich stellenweise durchaus Vorbildcharakter. Durch die Konzipierung als Nutzerkontrolliertes Identitätsmanagementsystem können die Nutzer des Portals jederzeit einsehen und kontrollieren, welche Daten wie auf der Plattform verarbeitet werden und wer, wann auf die Daten Zugriff hat. Auch wenn die Prüfung der technischen Implementierungsdetails auf der Ebene des Programmcodes nicht Gegenstand dieser Untersuchung sind, ist doch festzustellen, dass die Tatsache, dass das System als offene Software umgesetzt wurde, zusätzliches Vertrauen bilden kann. Ebenso ist die Tatsache, dass für den Betrieb ein Konsortium gewählt wurde, das sich aus verschiedenen Stakeholdern zusammen setzt und das Konsortium keine Gewinnerzielungsabsicht hat, ein weiterer Vertrauensanker.

Naturgemäß hat die hier vorgenommene umfassende Untersuchung einige Verbesserungsvorschläge aus datenschutzrechtlicher Sicht hervorgebracht, die der angefügten Tabelle 2 entnommen werden können. Alle Punkte sollten sich für die Betreiber gut umsetzen lassen und stellen keinesfalls Hinderungsgründe für den weiteren Betrieb auch mit Adressaten in Deutschland dar.

Eine Ausnahme hierzu wird jedenfalls dann bestehen, wenn ein Arbeitgeber eine Wissenschaftlerin oder einem Wissenschaftler zur Nutzung des ORCID Portals im Rahmen des Arbeitsverhältnisses verpflichtet.[84] In diesen Fällen ist die Freiwilligkeit der Einwilligung (der Wissenschaftlerin oder Wissenschaftlers) und damit die Rechtsgrundlage für einen Datentransfer durch ORCID (zumindest auch) ins außereuropäische Ausland zweifelhaft. Insbesondere vor dem Hintergrund des derzeit nach wie vor unglücklich gelösten Rechtsregimes zur Verarbeitung personenbezogener Daten in den USA kann bezüglich der Rechtmäßigkeit solcher Konstellationen derzeit keine risikofreie Prognose abgegeben werden. Dennoch können die rechtlichen Risiken auch für diesen Fall durch die in der Tabelle beschriebenen Maßnahmen zumindest deutlich reduziert werden.

[84] Zur Problematik der Freiwilligkeit der Einwilligung in dauerhaften Abhängigkeitsverhältnissen (wie zum Beispiel dem Arbeitsverhältnis), die grundsätzlich und auch ohne ausdrückliche Verpflichtung aufgrund des Machtgefälles zwischen den Parteien zweifelhaft ist vgl. Meike Kamp, Martin Rost, “Kritik an der Einwilligung”, DuD 2013, 80-84.

Ob es möglich bzw. erstrebenswert ist, ORCID in der Zukunft in ein distribuiertes oder dezentrales Modell zu überführen – was aus Datenschutzsicht Vorteile bieten kann – muss zukünftigen Untersuchungen vorbehalten bleiben. Hierfür bedarf es zunächst entsprechender Erfahrungswerte, für die das Portal eine sehr gute Grundlage bieten kann.

Bereich	
Empfehlung	**Seite**
Personenbezug	
1. Beschränkung der IP-Adressen von Lesenden	24
2. Auswertung der Nutzungsdaten von Lesenden in Bezug auf Profilinhaber	24
3. Audit der Anonymisierung	24
Rechtsgrundlage Einwilligung	
4. Voreinstellung / Privacy-by-default	30
Rechtmäßigkeit Auftragsdatenverarbeitung	
5. Seitens der datenverarbeitenden Stellen: Auftragsdatenvereinbarung schließen	30-34
6. Seitens ORCID: Muster für eine Auftragsdatenvereinbarung	30-34
7. Auditierung der technisch-organisatorischen Maßnahmen und Zertifizierung derselben	30-34
8. Erneute Prüfung der Möglichkeit einer Selbstverpflichtung nach den EU-US-Privacy-Shield-Regelungen	30-34
Transparenz / Privacy Policy	
9. Gesonderte Hinweispflicht auf Widerrufsmöglichkeit für die E-Mail-Adressen	35
10. Gesonderte Hinweispflicht auf Widerrufsmöglichkeit, wenn Profile auf Grundlage der Nutzungsdaten für Marketingzwecke § 15 Abs. 3 TMG	37
11. Deutsche Fassung der Privacy Policy vorhalten	37
Datensicherheit und Kontrolle	
12. Auditierung der Datensicherheit (wie oben)	37-39
13. Bestellung eines Datenschutzbeauftragten	38
Zweckbestimmung	
14. Klarstellung in Privacy Policy, welche Nutzungsdaten konkret für Identitätsmanagement verwendet werden	40-41
15. Prüfung der Erforderlichkeit bei Verwendung der Nutzungsdaten für Evaluierung (inkl. Anonymisierung, s.o) sowie Klarstellung, dass Nutzungsdaten nur insofern verwendet werden	40-41
16. Prüfung der Zweckvereinbarkeit neuer (bisher nicht in der Privacy Policy vorgesehener) zu späteren Zeitpunkt, sobald solche feststehen	48

Tabelle 2: Empfehlungen