ORCID aus datenschutzrechtlicher Sicht

ORCID from a data protection perspective*

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

[Expert opinion on behalf of the German Research Foundation (DFG) as part of the project ORCID DE for the promotion of the Open Researcher and Contributor ID in Germany]

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

Berlin im Mai 2017

This legal report is accessible online at http://doi.org/10.2312/lis.18.02

* This version of the report is partially translated, English parts are highlighted in yellow. The original German version is accessible online at http://doi.org/10.2312/lis.17.02
Unfortunately, the external translation resulted in a number of formatting errors, which could not be corrected with reasonable efforts.

Table of Contents

Einleitung [Introduction]

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]

Introduction – Translated Summary

This assessment focuses on how ORCID will be implemented in scientific institutions in Germany. In doing so, the institutional rules and German and European standards to which the scientific institutions in Germany which implement ORCID are subject, will be considered. In the process, account should be taken of the fact that personal data being collected in the European Union will be transferred into the USA. The key requirement of this assessment is that the assessment be formulated such that it is as generally understandable and universally applicable as possible, thus offering a guiding framework for legal evaluation onsite, for example in colleges and non-university research institutions. The concern of the assessment is to support scientific institutions in the legally compliant implementation of author identification using ORCID.

[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.

The preparation of the assessment was preceded by a process which ought to ensure cooperation with the DFG Project ORCID DE. Specific questions were compiled in this manner (Annex I)[14] during a workshop in 2016 after a presentation of fundamental data protection principles; further issues were addressed within the scope of an additional “Community Input” (Annex II), which was gathered by the project ORCID DE.

Also, part of the assessment was a correspondence with the operators of ORCID. The corresponding questions of this exchange are also addressed in this assessment.

[14] Annex I and Annex II are not contained in the publicly available version of this assessment for data protection law and copyright law reasons.

[15] S.o.

I. Method and Course of the Analysis

The methodology toolbox for data protection consulting contains a variety of approaches. In addition to the typical legal assessment of the documentation of processing activities, conducting Data Protection Impact Assessments, developing data protection concepts or developing a data protection management system, Privacy by Design can be taken into account. Beside such specific approaches, classic legal methodology, i.e., case-based examination of application scenarios can be applied. Finally, data protection regularly touches on questions of process organisation, ethical issues and those which have not (yet) been integrated into the law owing to the dynamic of their recent developments. Since, as a general rule, a multitude of interests and fundamental rights must be considered, risk assessments play a key role in almost all methods.

Structuring along application or usage scenarios seemed sensible for addressing the data protection law questions posed. This approach is especially well suited as an abstraction of the legal examination for the present questions. As ORCID‘s technical system is largely defined, retroactive technological approaches are to a great extent not at the centre of the analysis. However, ORCID‘s system provides several significant mechanisms which afford the user an extensive control over data management. Accordingly, the abstracted legal examination can provide useful pointers concerning the extent to which the existing system meets legal requirements. In this sense, the legal analysis can in particular reveal whether the correct risk considerations were made in the design. Ultimately, the case-oriented approach also makes sense because data protection’s principle of purpose limitation follows a similar structure. In addition, technical systems are often developed along what are referred to as “Use Cases”, which in turn conforms in the broadest sense to the application scenarios at issue here. However, references are also made to other methods in some places. [16]

[16] We note that this assessment cannot reproduce a full legal examination of all specific uses of ORCID. Likewise, it cannot provide a “clearance certificate under data protection law”. If possible at all, this must be reserved for other methods. An example is the EuroPriSe privacy seal. This offers a methodology that moves in this direction; however, this seal of approval also only allows the claim that a technology can be used in a way that fundamentally conforms to the law. Alternatively or additionally, what should also be considered is a prior check that is legally prescribed for data processing which bears high risk for those concerned.

In this report, we consider the functionalities of ORCID within the framework of the research subject (II.), clarify relevant questions of data protection law (III.), and consider certain legal questions more precisely (IV.). Finally, the Conclusion (V.) also contains recommendations that could arise for the further development of the platform.

Increasingly, this will be conducted by organisations for the sake of routine, even if the risk is not to be qualified as high – as is also true in the case of ORCID. This assessment can be consulted as a supplement within this framework, but – for want of knowledge concerning the specific processes and lack of insight into the specific technical implementations in or with ORCID – it cannot completely replace a prior check.

II. Untersuchungsgegenstand [Object of Investigation]

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.).

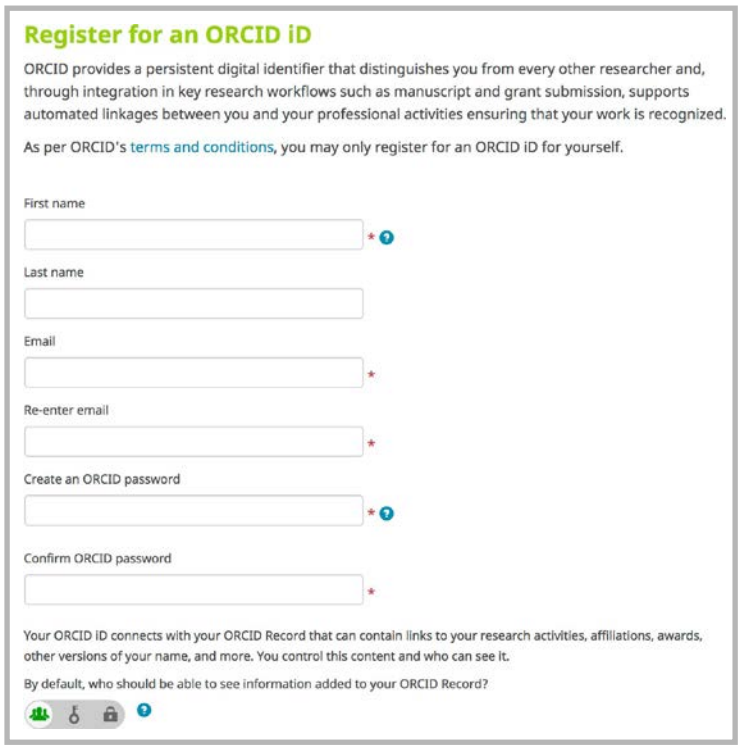

Abbildung 1: Registrierung

1. Anlegen eines ORCID-Profils [Instantiation of ORCID-profile]

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 [Privacy functionality: defaults]

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]

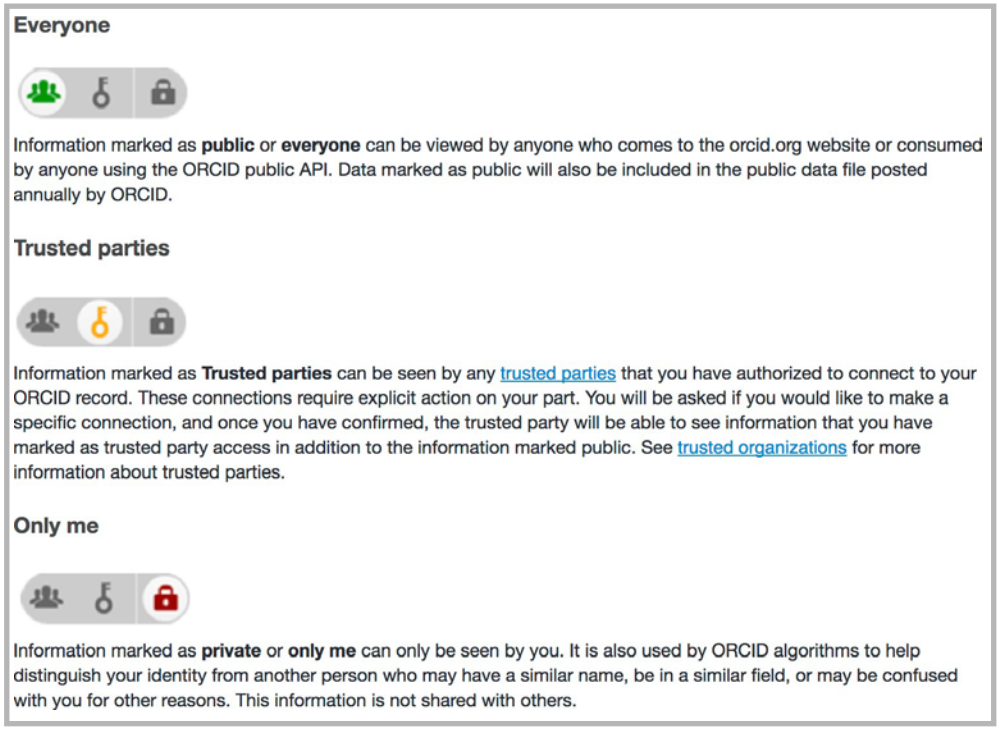

Abbildung 2: Datenschutz-Einstellungen

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 [Consent]

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]

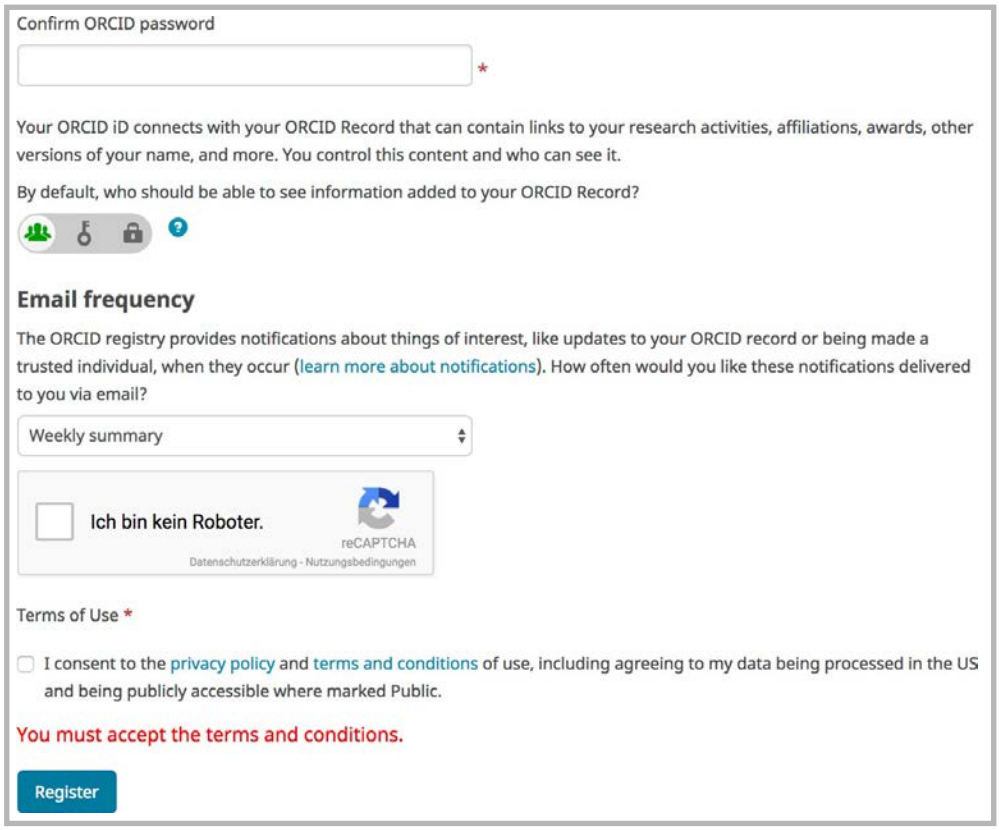

Abbildung 3: Einverständnismechanismus

2. Erstellung und Bearbeitung des ORCID-Profils [Editing of profiles]

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 [Data categories]

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 [Privacy functionality: specific settings]

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).

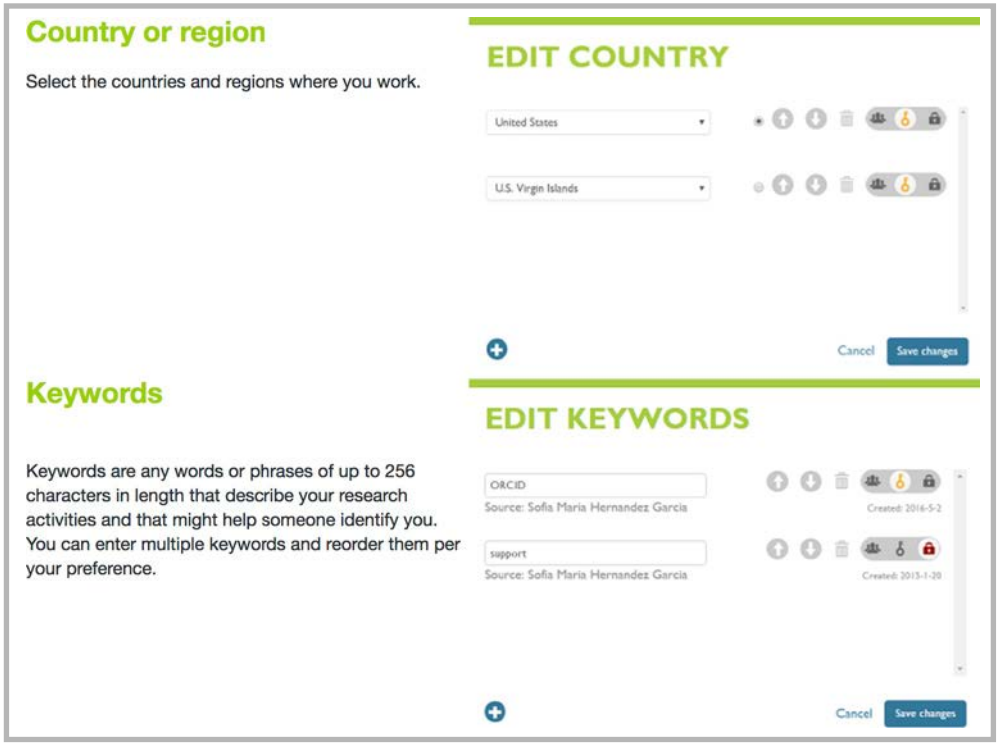

Abbildung 4: weitere Einstellungen

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“ [Delegation of administration to 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 [Administration of profile-data]

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 [Usage scenario: 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“ [Usage scenario: 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“ [Usage scenario: public access]

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 [Other functionalities]

a) ORCID als Identitätsmanagementsystem für Authentifizierungszwecke (Single-Sign-on via ORCID) [ORCID for Identity Managemement and authentication purposes]

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 [Future purposes]

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 [Conclusion]

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. General Data Protection Considerations

The objective of the legal analysis in this section is to conduct a data protection assessment of central functionalities of the ORCID platform for individuals and organisations in Germany. To this end, the data protection provisions under German law are currently relevant, particularly the *Bundesdatenschutzgesetz* [German Federal Data Protection Act (BDSG)]. As already mentioned at the start, the underlying EU General Data Protection Regulation (hereinafter also: GDPR) applicable on 28 May 2018 is also referred to at the relevant places in the following.

The subject-matter of this assessment is an electronic information and communication service. It is neither a telecommunications service nor a telecommunications-supported service in terms of the Telecommunications Act, nor is it a broadcast in terms of the Broadcasting Treaty. Hence, it is a telemedia service. Therefore, provided a corresponding regulation emerges, the special regulations of the *Telemediengesetz* [German Telemedia Act (TMG)] are to be observed, as well. They precede the BDSG regulations in this respect (*lex specialis*), § 1 para. 3 p. 1 BDSG.

These regulations will largely be replaced when the already-adopted European General Data Protection Regulation applies in May 2018 and will be broadly superseded by the ePrivacy Regulation which currently exists only in draft form.[42] Unlike the former EU provisions, which were adopted as directives that required implementation by means of national laws, the amendments are regulations and thus apply directly. Even so, clarifications and exceptions may or must be made by national legislators in a number of places (particularly within the framework of Art. 89 GDPR for scientific purposes in the public interest). At the time of the assessment, only a draft bill exists in Germany with regard to the GDPR; with respect to the ePrivacy Regulation, it is yet to be seen whether and to what extent any national leeway for implementation exists and will be used.

Therefore the assessment examines ORCID against currently applicable data protection law. To date there are only a few indications that the result of the legal assessment would fundamentally change due to the amendments. It is mentioned in the text where impacts are already discernible.

[42] Regulation (EU) 2016/679 of 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 the following general assessment of the compliance of the object of evaluation with data protection law, the scope of application (1.) and the regulation addressee (2.) should first be described in detail to then enable a first legal classification of the platform by means of fundamental data protection law principles of lawfulness (3.), purpose limitation and necessity (4.) as well as the supporting requirements of transparency, (data) security and further control mechanisms (5.).

It should be noted that the data protection law often allows ample room for interpretation and that no settles case law exists with regard to a multitude of legal questions. Therefore, the legal assessment cannot always be reliably assured but rather only points out legal risks. Opinions of supervisory authorities and the relevant literature provide orientation in these cases in addition to the classic legal methods of interpretation.

1. Anwendungsbereich: Personenbezogene Daten [Scope: personal data]

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 [Registration, profile and usage data of (logged-in) users]

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) GDPR, 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 [Usage data of not-logged-in users]

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 [Identification of registered users wrt to anonymised usage data]

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 [Anonymisation of personal data]

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 [Interim Conclusion]

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. Regulationsadressat: Verantwortliche Stelle [Data Controller]

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 GDPR (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 GDPR Auftragsdatenverarbeiter, „eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet“.

a) ORCID as the Responsible Body under Data Protection Law

In the first situation considered, wherein scientists create and maintain their profile independently and in their own interest, ORCID is to be viewed as the data controller and thereby is responsible body as well, according to both definitions. This applies both to the different categories of data and to the different purposes for which ORCID processes this data. Hereinafter, a fundamental difference is made between the following processing purposes of ORCID:

- ORCID initially collects and processes registration, profile, and usage data from profile users to facilitate their distinct worldwide identification within scientific systems and the attribution of their scientific works.
- In so doing, ORCID collects and processes this data particularly in order to maintain, evaluate and improve the portal and
- to contact the users, for example to notify them of changes in the Privacy Policy, to make contact with additional participants in the scientific system or for its own marketing activities.

ORCID is not the data controller for the data processing only if ORCID does not collect or process the data for its own purposes but instead acts on behalf of a third party and abides by these prescribed purposes. This might be the case, for example, if ORCID processes the data on behalf of an employer or user.

It does not matter for the application of data protection regulations that the operating company ORCID Inc. is based in the United States of America. According to § 1 para. 5 clause 2 BDSG, the data protection law is also applicable for companies, whose principal office is situated abroad, as it draws exclusively reflects on the domestic collection (in Germany), which is what is assumed for the situation studied here. According to the aforementioned standard, the case would only have to be assessed differently if the entity was located elsewhere in the European Union or in another contracting member state of the European Economic Area. In any event, pursuant to Art. 3 GDPR, the fundamental data protection regulation will also apply to the data processing described here when it becomes applicable.

b) Verantwortlichkeit weiterer Verwender der Daten [Responisibilities of others]

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 Requirements 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 [Interim Conclusion]

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 [Consent Requirements]

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 GDPR).

a) Grundsätzliche Requirements an die Einwilligung [Requirements of consent]

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 [Consent via opt-in]

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

- Soweit die regulations 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 regulations der ab März 2018 wirksamen GDPR 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 [Further transparency and control-mechanisms via privacy functionalities]

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) The Voluntary Nature of Consent in Special Situations (Particularly: Depiction of the Legal Situation in the Context of Data Transfer in the United States of America)

Normally, the voluntariness requirement can be met without a problem. However, this criterion can pose problems if an employer prescribes the use of ORCID.

As it is still currently imperative to scientific careers to publish through relevant specialised publishers, registration required by these publishers (or, more precisely:

[51] Siehe oben, Abbildung 2 und die zugehörigen Ausführungen.

[52] Hierdurch dürfte auch bereits die weitergehenden Requirements des Artikel 25 Abs. 2 GDPR, der datenschutzfreundliche Voreinstellungen vorschreibt, Rechnung getragen werden.

providing an ORCID iD, which requires registration) can raise doubts concerning voluntariness. Provided that there are no such dictates, however, it is to be assumed that consent is given voluntarily. In any case, it is worth to highlight that almost all scientific institutions already capture information such as publications and projects within the scope of their information management so that the information stored in ORCID can also be found elsewhere – often freely online.

It is a different case if an employer requires that an ORCID iD be set up. Here, it is not decisive whether an explicit instruction is given. By virtue of the power imbalance between employer and employee, it is to be assumed that voluntariness can no longer be implied if participation in the platform is implicitly expected. In these cases, the legal ground for the data processing can either be the respective employment contract, the operational practice – to be coordinated with the works council, where applicable – or the legitimate interests of the employer. This means that the processing of data is to be allocated to the respective institution in all of these cases. It thereby becomes the responsible body for data processing. As it does not itself conduct the data processing, this can only be based on the regulations concerning contractual data processing according to § 11 BDSG. However, the requirements described there must then be met. In particular, according to paragraph 2, a written order (contracted data processing) is to be placed with ORCID which is to consider the additional requirements listed in greater detail in paragraph 2. Alongside this exists a regular monitoring obligation with regard to the technical and organisational measures and the corresponding duty of documentation of the processor.

In practice, these listed requirements are regularly realised on the basis of standardised model contracts; relevant templates are offered by data supervision authorities, among others.[53] For simplification, it is recommendable that ORCID maintain an adapted model and offer it to relevant institutions as the basis for concluding a contractual data processing agreement.[54]

[53] Hessian Data Protection Officer (Ed.), Sample Agreement for Contractual Data Processing in accordance with § 11 BDSG, https://www.datenschutz.hessen.de/download.php?download_ID=239 (7.5.2017) or also at Datenschutz-Wiki, formerly operated by the Federal Commissioner for Data Protection and Freedom of Information (BfDI), now jointly operated by Ruhr University Bochum (RUB) and Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. [Data Protection Officer Trade Association of Germany] at https://www.datenschutzwiki.de/Mustervereinbarung_Auftragsdatenverarbeitung (7 May 2017).

[54] Google Inc., among others, has chosen a similar approach for running its Google Analytics service, cf. https://static.googleusercontent.com/media/www.google.de/de/de/analytics/terms/de.pdf (7 May 2017).

The control measures with respect to the technical and organisational measures of the processor must normally be carried out by the controller itself, i.e., in the case at hand the employer of the scientist. However, it is recognised that this can also be done by third parties on the basis of an appropriate auditing process. Such an auditing process can replace in particular an in-person inspection by the employer itself if it is based on a certificate pursuant to ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements.[55]

Here it is lastly to be taken into account that the contractual data processing is not conducted in an EU member state. According to § 4b para. 2 BDSG, transmission to places not stated in para. 1 (in particular, not located within an EU member state pursuant to para. 1 no.) is forbidden in particular if a reasonable level of protection is not guaranteed at this place. A presumption of a reasonable level of protection applies if the EU Commission has rendered a corresponding decision on adequacy pursuant to Art. 25 para. 1 Directive 95/46. Such a decision exists with respect to data processing in the United States ("EU-US Privacy-Shield").[56] According to this, the Commission comes to the conclusion that the United States guarantees an adequate level of protection for personal data within the framework of the EU-US-Data Protection Shield from the European Union to self-certified organisations." (Clause 13 in the German translation, sic!).

Even if the final, meaningful verb is missing from the corresponding crucial sentence in the German language, the English language version, as well as the interpretation, show that it is intended that self-certified organisations attain a reasonable level of protection according to the rules which are further elaborated.[57]

[55] See Datenschutz-Wiki: https://www.datenschutz-wiki.de/Auftragsdatenverarbeitung (7 May 2017); Spindler/Schuster, "Recht der elektronischen Medien" [Law of Electronic Media], 3rd ed. 2015, BDSG § 11, marg. No. 22. However, often it is not sufficiently observed in the technical literature that this can only hold true if the corresponding certification is also conducted with a comprehensive scope, cf. ISO (ed.), "ISO/IEC 27001:2013 *Information technology – Security techniques – Information security management systems – Requirements", p. 1, ("clause 4.3")*. The auditing process by TRUSTe may not satisfy the requirements, however, as it pertains to the Privacy Policy and not ORCID's technical and organisational measures.

[56] European Commision: Implementation Decision (EU) 2016/1250 by the Commission from 12 July 2016 pursuant to Directive 95/46/EG of the European Parliament and the European Council concerning the adequacy of the protection afforded by the EU-US data protection shield (Disclosed under File Number C(2016) 4176) (Text germane for the EEA. In: *Amtsblatt der EU, ABl. L 207 from 1 August 2016, p. 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 aims to comply with the requirements for such a self-certification, but as a non-profit organisation considers itself excluded from participation in the program because the United States Federal Trade Commission, which is responsible for oversight of the Privacy Shield, does not have jurisdiction over non-profits.[58] Accordingly, ORCID is not included on the Federal Trade Commission's list. [59] Thus, the presumption of an adequate level of protection on the basis of the EU decision mentioned does not apply for ORCID.

It cannot be definitively assessed whether the adequacy of the level of protection has been attained nevertheless. Doubt exists in particular because self-certification also stipulates an assurance of procedural guarantees – specifically subjection to arbitration. Generally, the Privacy Policy accordingly contains a reference to an arbitration board. [60] However, the extent to which the absence of a declaration to the Federal Trade Commission affects enforceability cannot be clearly assessed.[61] Moreover, the EU Parliament has also articulated doubts with respect to the legal strength of the Privacy Shield decision which not least also center on the issue that parties concerned do not have any legal protections that are comparable to EU standards. [62]

Particularly in the case where an employee of a German university is prompted by his employer to participate in ORCID, he – in the case of conflict – has a considerably more cumbersome and very likely less effective means of recourse than if the processing were to take place within the EU such that certain doubts arise as to the adequacy of the level of protection. However, nor is the enforcement of data protection rights within Europe trivial by any means, such that a final assessment of the various (actual) levels of protection cannot be made here. For the institution that entrusts ORCID with the administration of its employee data, a certain risk remains that this data processing will be considered impermissible. However, it is to be stressed that, provided only publicly available information is displayed, the risk for the parties concerned and thus the potential for damages would be quite low.

---

[58] Point 12.0 of the Privacy Policy.

[59] Federal Trade Commission (ed.) https://www.privacyshield.gov/list (7 May 2017).

[60] Point 12.0 and 13.0 of the Privacy Policy.

[61] For example the Federal Trade Commission Act, which clearly authorises the Federal Trade Commission to impose sanctions in cases of contravention of the self-certification statements, cf. https://www.export.gov/article?id=Enforcement-of-Privacy-Shield (7 May 2017).

[62] European Parliament, "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))", no. 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) referring to similar doubts on the part of the European data protection authorities (Article 29 Group) in lit H.

In summary, it is recommended that institutions wishing that their employees set up an ORCID iD conclude a corresponding data processing agreement with ORCID. It is recommended that ORCID provide a standard text for this purpose and have the technical and organisational measures audited externally. Finally, it would be necessary to re-examine whether it really is not possible for ORCID to make a relevant Privacy Shield-compliant self-commitment to the responsible Department of Commerce and consequently be able to benefit from the presumption of an adequate level of protection on the basis of the corresponding Commission decision (see above). In addition, it is recommended that the organisations concerned monitor the further discussion and case law closely and modify their practice, if necessary. Due to the complexity of the data protection law and the low level of permeation by the case law, it must be noted that a legal risk cannot be ruled out, even considering all recommendations.

e) Rechtsgrundlage und Widerspruchsmöglichkeit für Speicherung der E-Mail-Adresse für die Zeit nach Löschung des Profils [Lawfulness and objection wrt to processing of email-Adress for the time after deletion of the profile]

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 Requirement 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) Interim Conclusion

A legal basis exists, in principle, for the processing of personal data. The processing of registration, profile and usage data by ORCID Inc. can be based on an effective declaration of consent. With regard to the profile data, the privacy functionality with its extensive transparency and control options constitutes an exemplary implementation of the privacy by design approach. The continued storage of e-mail addresses can potentially be based on the legal provision for the “legitimate interests” of the controller. It is also revocable, which is to be emphasised in the Privacy Policy.

4. Prinzipien der Zweckbindung und Erforderlichkeit [Principles of purpose limitation and necessity]

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 [Transparency, Security, and Control]

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

a) Transparenz [Transparency]

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 Requirements 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 über- prüft werden kann, ist damit also der Requirement 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 Requirement 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 Requirements 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 Zertifikatstandards 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 Transparenzrequirements des TMG sind bei ORCID eingehalten, allerdings ist zu empfehlen auch eine deutsche Fassung der Privacy Policy vorzusehen.

b) Sicherheit [Security]

Requirements 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 GDPR, 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 [Control]

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 GDPR diese Schwellwerte maßgeblich modifiziert. Nach Art. 37 Abs. 1 GDPR müssen der Verantwortliche (aber auch der Auftragsdatenverarbeiter) nur dann einen Datenschutzbeauftragten bestellen, wenn die verarbeiteten Daten gemäß Art. 9 GDPR 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 GDPR 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) Interim Conclusion

No conflicts are discernible with respect to the data protection law requirements in the areas of transparency, security and control mechanisms; small readjustments are recommended, however. The privacy statement should also be provided in German. Technical security could also be verified by an external audit or certification and a data protection officer with a sufficient degree of independence should be appointed.

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

IV. Zweckbindung und Erforderlichkeit einzelner Nutzungsszenarien [Processing of User Data]

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 [Processing purposes of 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 [Processing of registration and profile data for the purpose of Identity Management]

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 [Processing of usage data for the purpose of Identity Management]

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 [Processing of usage data for the purpose of maintenance, evaluation and improvement of the 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 [Processing of registration data for direct contact]

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) Interim Conclusion

The purposes of processing registration and profile data for identity management by ORCID can be adequately determined by means of the context (also by the users of the portal). The processing of registration information is required for these purposes. The standard storage of e-mail addresses for the time after the profile is deleted is also considered necessary insofar as this is supposed to preserve the opportunity for the user to revive his or her profile at a later date (in addition, the users of the portal can object to the continued storage at any time). The processing of profile information is also required for identity management. However, the necessity for data labelled as “private” for these purposes is to be examined closely in the individual case. A clarification should be made in the Privacy Policy insofar as usage data is not used for purposes of identity management.

The question whether the processing of user data for purposes of maintenance, evaluation and improvement of the platform meets the necessity requirement depends largely on the anonymization technology used. This is to be examined closely in the individual case. It should be clarified in the Privacy policy that the user data is not used beyond this.
Finally, registration data for making contact is processed for sufficiently specific purposes. Processing is also necessary in this respect.

2. Verarbeitung durch Dritte zu eigenen Zwecken [Processing by Third parties]

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 Requirements hinausgehen) [No legal responsibility for ORCID (mechanisms extending beyond legal requirements]

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) [Processing of „limited-access"-data by trusted organisations (esp. transmission to third parties for marketing purposes]

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. „regulationsadressat: Verantwortliche Stelle".
[80] Siehe hierzu bereits oben unter Punkt IV. 2. „regulationsadressat: 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 [processing of public data by anyone]

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) Interim Conclusion

ORCID does not act as a (responsible) controller as long as it processes personal data exclusively pursuant to purposes determined by third parties. Thus, a user of the portal bears the responsibility himself insofar as “Trusted Individuals” exclusively pursue aims by means that are prescribed to them by the user. Unlike “Trusted Individuals”, “Trusted Organisations” and other third parties process the personal data at least for their own purposes as well. Provided that the data is processed exclusively for such (own) purposes, they are the (responsible) controller under data protection law.

3. New Processing Purposes

The processing of personal data for new purposes, i.e. for purposes other than what was specified when it was collected, requires a new legality assessment. The purpose limitation principle does not prohibit the further processing of personal data for other purposes per se.

---

[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.

It instead requires either a proportionality test (in German law) or a purpose compatibility test (in European law).

a) Deutsche Rechtslage [German legal environment]

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 regulation 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) European Legal Situation

In European law, a change in purpose is lawful if the new purpose is not incompatible with the original purpose, Art. 6 para. 1 lit. b Directive95/46/EC. The same applies pursuant to Art. 5 para. 1 lit. b GDPR, whereby

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

Art. 6 para. 4 clarifies according to which criteria such a purpose compatibility test is to be conducted. According to this, the focus is the connection between the different purposes; the context in which the data was collected; the type of personal data; the potential consequences for the parties concerned as well as the presence of appropriate safeguards such as encryption or pseudonymisation of the data.

Art. 89 GDPR earmarks what is referred to as a flexibility clause for processing for archiving purposes which are in the public interest, for scientific or historical research purposes and for statistical purposes. According to this, the member states can, conditional upon certain guarantees, make exceptions to certain rights and guarantees. As already mentioned above, there only exists one draft bill to date.

c) Interim Conclusion

Absent additional reference points, the legality of new purposes (not examined in this assessment) can only be delineated according to fundamental legal principles. In detail, the examination of legality must therefore be conducted in each specific case.

V. Conclusion and Recommendations

The assessment of ORCID pursuant to data protection law could not find any serious shortcomings. To the contrary, with its privacy functionalities, the system supports users' exercising their rights to informational self-determination and in places definitely has an exemplary character with respect to this.
With its nature as a user-controlled identity management system, users of the portal can see and control at any time what data is processed on the platform and who has access to the data at which time. Even though the examination of the technical implementation details on the level of the program code is not the subject of this analysis, one must notice that the fact that the system is implemented as open software can build additional trust. Likewise, trust is also rooted in the fact that a consortium consisting of various stakeholders was selected for the operation and that the consortium does not aim to make a profit.

Naturally, the comprehensive analysis conducted here spawned several suggestions for improvement from a data protection law perspective, which can be extracted from Table 2, attached. It should be feasible for the operators to implement all points and in no way present obstacles to continued operation, with recipients in Germany.

There is an exception to this in any case if an employer compels a scientist to use the ORCID portal within the scope employment relationship.[84] In these cases, the voluntary nature of the consent (from the scientist) and therefore the legal basis for a data transfer by ORCID to a non-European foreign country is (also) questionable. In particular, given the current unfortunate legal treatment of the processing of personal data in the United States, a risk-free forecast cannot be made at this time with respect to the lawfulness of such situations. Nevertheless, the legal risks can at least be reduced significantly for this case, as well, with the measures described in the table.

[84] Concerning the issue of the voluntary nature of consent in lasting dependent relationships (such as the employment relationship), which is questionable generally and also devoid of an express commitment due to the imbalance of power between the parties cf. Meike Kamp, Martin Rost, "Kritik an der Einwilligung" [Critique of Consent], 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.

Area Recommendation	Page
Personenbezug	
1. Storage limiation for IP-Addresses wrt read-access	24
2. Processing of usage data of read-access wrt profiles	24
3. Auditing anonymisation functions	24
Legality of consent	
4. Privacy-by-default	30
Legality of proccessing (Art. 28 GDPR)	
5. Wrt to controllers: contract obligation	30-34
6. Wrt ORCID: Provide sample contract	30-34
7. Audit of technical and organisational measures and certification thereof	30-34
8. Reconsider self-certification according to the EU-US-privacy shield mechanism	30-34
Transparency / Privacy Policy	
9. Explicit notification of right to withdraw consent wrt e-mail-addresses	35
10. Explicit notification of right to withdraw consent wrt usage data for marketing purposes according to § 15 Abs. 3 TMG	37
11. Provide a german version of the Privacy Policy	37
Data security and control	
12. Audit of data security (see above)	37-39
13. Designation of a data protection officer	38
Purpose limitation	
14. Clarification in privacy policy wrt to the question which usage data are necessary for identity management purposes	40-41
15. Reassessment of necessity of usage data for evaluation purposes (incl. anonymisation, see above) and clarification that the data is exclusively used for this purpose	40-41
16. Assessemen of compatibility of future purposes (not yet declared in the privcy policy), before using data for such purposes	48

Table 2: Recommendations