PANELFIT

PARTICIPATORY APPROACHES TO A NEW ETHICAL AND LEGAL FRAMEWORK FOR ICT

Verhaltenskodex zum Datenschutz für verantwortungsvolle Forschung und Innovation

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document reflects only the authors' view and the Agency is not responsible for any use that may be made of the information it contains.

An dem Dokument beteiligte Projektpartner

Nr.	Name der teilnehmenden Organisation	Abkürzung
1	Institut de Ciències del Mar (Consejo Superior de Investigaciones Científicas)	ICM-CSIC
2	Universidad del País Vasco / Euskal Herriko Unibertsitatea	UPV/EHU
3	European Network of Research Ethics Committees	EUREC
4	Unabhängiges Landeszentrum für Datenschutz AöR	ULD
5	Österreichische Akademie der Wissenschaften	OEAW
6	Fonden Teknologiradet	DBT

Dokumentenhistorie

Status	Version	Datum	Autor(en)	Überprüft von
Entwurf	v0.5	2020-10-30	Pranesh Prakash (ICM-CSIC)	Karen Soacha (ICM-CSIC), Jaume Piera (ICM-CSIC)
Entwurf	v1.0	2020-11-03	Pranesh Prakash (ICM-CSIC)	Julia Maria Mönig (EUREC), Johann Cas (OEAW), Bud Bruegger (ULD), Harald Zwingelberg (ULD), Bjørn Bested (DBT)
Entwurf	v2.0	2020-12-06	Pranesh Prakash (ICM-CSIC)	Iñigo de Miguel Beriain (UPV/EHU), Karen Soacha (ICM-CSIC)
Entwurf	v3.0	2021-01-23	Pranesh Prakash (ICM-CSIC)	Karen Soacha (ICM-CSIC)
Endgültige Version	v4.0	2021-08-02	Pranesh Prakash (ICM-CSIC)	Karen Soacha (ICM-CSIC), Iñigo de Miguel Beriain (UPV/EHU)

Inhaltsverzeichnis

1 Präambel

Dieser Verhaltenskodex zum Datenschutz für verantwortungsvolle Forschung und Innovation (CCDP) ist ein Beitrag des PANELFIT-Projekts für die Forschungsgemeinschaft.

PANELFIT (Participatory Approaches to a New Ethical and Legal Framework for ICT) ist ein unter Horizon 2020 finanziertes Projekt, das operative Standards und praktische Leitlinien zur Lösung einiger ethischer und rechtlicher Fragen im Zusammenhang mit IKT-Technologien erarbeitet hat. Das Projekt PANELFIT soll somit Klarheit und Leitlinien in Bezug auf die Fragen an der Schnittstelle zwischen verantwortungsvoller Forschung und Innovation,1 Ethik und Datenschutz schaffen.

Der CCDP zielt darauf ab, eine leicht verständliche Reihe von Verhaltensregeln bereitzustellen, die die wichtigsten Grundsätze der Datenschutz-Grundverordnung (DSGVO) der EU abdecken, sowie eine Reihe von unerwünschten Praktiken aufzuführen, die speziell auf die Forschungsgemeinschaft zugeschnitten sind.2 Es gibt mehrere Verhaltenskodizes für verantwortungsvolle Forschung und Innovation. Diese bestehenden Verhaltenskodizes enthalten jedoch keine Leitlinien zu den Datenschutzgrundsätzen, eine Lücke, die der CCDP zu schließen versucht. Der CCDP versteht sich als Einführung in die Datenschutzgrundsätze und versucht nicht, alle Aspekte der DSGVO abzudecken, die für Forscher von Belang sein könnten. So zielt der CCDP zum Beispiel nicht darauf ab, alle eventuellen Pflichten von Forschern gemäß den Datenschutzgesetzen oder alle Rechte von Einzelpersonen, deren personenbezogene Daten von Forschern verwendet werden, bzw. die rechtlichen Anforderungen in Bezug auf den Austausch personenbezogener Daten mit Forscherkollegen außerhalb der EU, Datenschutzgesetze auf nationaler Ebene und so weiter, abzudecken. Das PANELFIT-Projekt hat auch „Leitlinien zu datenschutzrechtlichen, ethischen und rechtlichen Fragen in der IKT-Forschung und -Innovation“ erstellt, die in dieser Hinsicht viel umfassender sein sollen.

1Verantwortungsvolle Forschung und Innovation (Responsible Research and Innovation, RRI) ist ein wichtiger Bestandteil des Programms „Wissenschaft mit der und für die Gesellschaft“ im Rahmen von Horizont 2020 (H2020) der EU. „Verantwortungsvolle Forschung und Innovation ist der fortlaufende Prozess der Ausrichtung von Forschung und Innovation an den Werten, Bedürfnissen und Erwartungen der Gesellschaft.“ („Erklärung von Rom über verantwortungsvolle Forschung und Innovation in Europa“). Die Europäische Kommission stellt fest, dass „RRI ein integrativer Ansatz für Forschung und Innovation (F&I) ist, um sicherzustellen, dass die gesellschaftlichen Akteure während des gesamten Forschungs- und Innovationsprozesses zusammenarbeiten … Allgemein ausgedrückt bedeutet RRI, dass potenzielle Auswirkungen und gesellschaftliche Erwartungen in Bezug auf Forschung und Innovation vorausgesehen und bewertet werden.“ (Europäische Kommission, „Wissenschaft mit der und für die Gesellschaft”)

2 Auch wenn es keine einheitliche, allgemein akzeptierte Definition von Forschung gibt, sollte man sich die Worte des Europäischen Datenschutzbeauftragten in einem kürzlich veröffentlichten Bericht vor Augen halten: „Seriöse Definitionen von Forschung betonen in der Regel systematische Tätigkeiten, einschließlich der Erfassung und Analyse von Daten, die den Bestand an Verständnis und Wissen sowie deren Anwendung erhöhen. Die Europäische Kommission hat die Ziele der Forschung und Richtlinien der EU wie folgt definiert: „Öffnung des Innovationsprozesses für Menschen mit Erfahrung in anderen Bereichen als den Hochschulen und der Wissenschaft“, „Verbreitung von Wissen, sobald es verfügbar ist, unter Verwendung digitaler und kollaborativer Technologien” und „Förderung der internationalen Zusammenarbeit in der Forschungsgemeinschaft“.“ (Europäischer Datenschutzbeauftragter, „A Preliminary Opinion on Data Protection and Scientific Research“, 9–10))

1.1 RRI und Datenschutz

Forschungstätigkeiten, sei es in der Forschung oder bei der Verbreitung von Forschungsergebnissen, sind oft mit personenbezogenen Daten anderer Personen verbunden.3 Die Datenethik ist somit ein notwendiger Bestandteil einer verantwortungsvollen Forschung und Innovation, und dazu gehört auch der Schutz personenbezogener Daten. In der EU ist der Schutz personenbezogener Daten ein Grundrecht, das in der Charta der Grundrechte der Europäischen Union verankert ist. Die Datenschutz-Grundverordnung stellt in diesem Sinne konkrete rechtliche Leitlinien in Bezug auf dieses Recht bereit.

Wenn Forscher personenbezogene Daten verarbeiten, müssen sie sich an die Datenschutzgesetze halten und sollten sich bemühen, bewährte Datenschutzpraktiken anzuwenden.

Der CCDP soll es Forschern erleichtern, die Grundprinzipien des europäischen Datenschutzrechts zu verstehen, und ihnen das Wissen vermitteln, wie sie diese Prinzipien im Rahmen einer verantwortungsvollen Forschung und Innovation praktisch anwenden können. Das Verständnis von Forschung im Rahmen der DSGVO ist weit gefasst und deckt Tätigkeiten ab, die Wissen bereitstellen, das „die Lebensqualität zahlreicher Menschen verbessern und die Effizienz der Sozialdienste verbessern kann“, und schließt „die technologische Entwicklung, die Grundlagenforschung, die angewandte Forschung und die privat finanzierte Forschung sowie Studien ein, die im öffentlichen Interesse im Bereich der öffentlichen Gesundheit durchgeführt werden“.4

3 Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Der Begriff ist sehr weit gefasst und umfasst den Namen einer Person, ihre Identifikationsnummer, Standortdaten, eine Online-Kennung oder Faktoren, die sich auf die physische, physiologische, genetische, mentale, wirtschaftliche, kulturelle oder soziale Identität dieser Person beziehen.

4 Datenschutz-Grundverordnung, Verordnung (EU) 2016/679, Erwägungsgrund 159.

2 Datenschutzgrundsätze

Der Schutz personenbezogener Daten nach der DSGVO beruht auf einer Reihe von Grundsätzen:

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz5
- Zweckbindung6
- Datenminimierung7
- Richtigkeit8
- Speicherbegrenzung9
- Integrität und Vertraulichkeit10
- Rechenschaftspflicht11

2.1 Rechtmäßigkeit, Verarbeitung nach Treu und Glauben sowie Transparenz

Um die Anforderungen des Grundsatzes der Rechtmäßigkeit, Verarbeitung nach Treu und Glauben und Transparenz zu erfüllen, müssen Forscher:

- den Zweck der Erhebung und Verwendung personenbezogener Daten bestimmen;
- sicherstellen, dass sie einen gültigen Grund (mindestens einen der sechs in der DSGVO genannten Gründe („Rechtsgrundlagen“) für die Erhebung und Nutzung der Daten bestimmen;
- sicherstellen, dass alles, was sie mit den Daten tun, rechtmäßig ist und im Einklang mit allen geltenden Gesetzen und ethischen Richtlinien steht, einschließlich derjenigen, die sich auf klinische Prüfungen, geistiges Eigentum, Menschenrechte, Verträge usw. beziehen;
- die Erwartungen der Personen hinsichtlich der Verwendung ihrer Daten durch die Forscher und was diese für angemessen halten würden ermitteln;
- die möglichen Schäden für die Personen, deren Daten verwendet werden, ermitteln;
- die Daten in einer offenen und transparenten Weise erheben und verwenden;

---

5 Datenschutz-Grundverordnung, Verordnung (EU) 2016/679, Art. 5 Absatz 1 Buchstabe a.

6 Datenschutz-Grundverordnung, Verordnung (EU) 2016/679, Art. 5 Absatz 1 Buchstabe b.

7 Datenschutz-Grundverordnung, Verordnung (EU) 2016/679, Art. 5 Absatz 1 Buchstabe c.

8 Datenschutz-Grundverordnung, Verordnung (EU) 2016/679, Art. 5 Absatz 1 Buchstabe d.

9 Datenschutz-Grundverordnung, Verordnung (EU) 2016/679, Art. 5 Absatz 1 Buchstabe e.

10 Datenschutz-Grundverordnung, Verordnung (EU) 2016/679, Art. 5 Absatz 1 Buchstabe f.

11 Datenschutz-Grundverordnung, Verordnung (EU) 2016/679, Art. 5 Absatz 2.

- die Personen in verständlicher Sprache darüber informieren, wer die Daten erhebt oder erhält, auf welcher Rechtsgrundlage sie erhoben/erhalten werden, warum sie erhoben/erhalten werden, wie lange sie aufbewahrt werden, wie und von wem sie verwendet werden und welche Rechte sie haben;
- die Daten auf eine Weise verwenden, die nach Treu und Glauben erfolgt, fair ist, den Erwartungen des Einzelnen entspricht und ihm keinen ungerechtfertigten oder unfairen Schaden zufügt;
- prüfen, ob sich die zu erhebenden Daten auf „besondere Kategorien personenbezogener Daten“ (sensible Daten laut der Definition der DSGVO) beziehen; in diesem Fall muss eine der in Art. 9 Absatz 2 DSGVO aufgeführten spezifischen Rechtsgrundlagen erfüllt sein, wie z. B. die ausdrückliche Einwilligung der betroffenen Person oder eine gesetzliche Grundlage, die eine solche Erhebung für „im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke“ erlaubt;
- prüfen, ob sich die zu erhebenden Daten auf „strafrechtliche Verurteilungen und Straftaten“ beziehen; in diesem Fall gelten besondere Gesetze.

Hintergrund

Nach europäischem Recht muss jede Verarbeitung personenbezogener Daten zu einem rechtmäßigen Zweck und mit einem legitimen Ziel erfolgen. Während die anderen Grundsätze die Art und Weise, wie personenbezogene Daten verarbeitet werden dürfen, einschränken, beschränkt dieser Grundsatz die Zwecke, zu denen personenbezogene Daten verarbeitet werden dürfen.

Rechtgrundlage

Die DSGVO legt sechs Grundlagen12 für die rechtmäßige Verarbeitung personenbezogener Daten fest. So muss der Zweck der Verarbeitung personenbezogener Daten unter mindestens eine der sechs Kategorien fallen:

- Einwilligung der betroffenen Person
- Erfüllung eines Vertrags
- Erfüllung einer rechtlichen Verpflichtung
- Erforderlich, um lebenswichtige Interessen einer Person zu schützen
- Erforderlich für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt
- Wahrung berechtigter Interessen

Es sei darauf hingewiesen, dass Behörden im Gegensatz zu privaten Einrichtungen kein „berechtigtes Interesse” als Zweck angeben dürfen, es sei denn, die Verarbeitung fällt nicht in den Aufgabenbereich der Behörde. Außerdem setzen „Einwilligung” und „öffentliches Interesse“ ein

12 Datenschutz-Grundverordnung, Verordnung (EU) 2016/679, Art. 5 Absatz 6.

„dringendes soziales Bedürfnis“ voraus, im Gegensatz zu weitgehend privaten oder kommerziellen Vorteilen.13

Wenn die „Einwilligung“ als Grundlage verwendet wird, ist es wichtig, dass der Zweck klar und ausdrücklich angegeben und in leicht verständlicher Form offenbart, erklärt oder ausgedrückt wird, warum die Daten erhoben und verarbeitet werden. Die Einwilligung selbst muss freiwillig, für einen konkreten Fall, nach ausreichender Information des Betroffenen und unmissverständlich abgegeben werden, und die Person hat das Recht, die Einwilligung jederzeit zu widerrufen.

Die DSGVO räumt ein, dass „der Zweck der Verarbeitung personenbezogener Daten für Zwecke der wissenschaftlichen Forschung zum Zeitpunkt der Erhebung der personenbezogenen Daten oftmals nicht vollständig angegeben werden kann. Daher sollte es betroffenen Personen erlaubt sein, ihre Einwilligung für bestimmte Bereiche wissenschaftlicher Forschung zu geben, wenn dies unter Einhaltung der anerkannten ethischen Standards der wissenschaftlichen Forschung geschieht. Die betroffenen Personen sollten Gelegenheit erhalten, ihre Einwilligung nur für bestimme Forschungsbereiche oder Teile von Forschungsprojekten in dem vom verfolgten Zweck zugelassenen Maße zu erteilen.“14

Der Europäische Datenschutzbeauftragte (EDSB) stellt fest, dass „die normalerweise nach der DSGVO für einen konkreten Fall erforderliche Einwilligung im Fall von erhobenen und hergeleiteten Daten und insbesondere im Fall von besonderen Datenkategorien, auf die sich ein Großteil der wissenschaftlichen Forschung stützt, weniger angemessen sein kann“. Wenn „die Forschungszwecke daher nicht vollständig konkretisiert werden können, würden von einem Verantwortlichen weitere Maßnahmen erwartet, um sicherzustellen, dass der Kern des Rechts der betroffenen Person auf eine gültige Einwilligung gewahrt wird, einschließlich durch so viel Transparenz wie möglich und andere Garantien“.15

Verarbeitung nach Treu und Glauben

Außerdem muss die Art der Verarbeitung nach Treu und Glauben erfolgen und transparent sein. Selbst wenn die Verarbeitung auf einer rechtmäßigen Grundlage durchgeführt wird, kann sie dennoch nicht nach Treu und Glauben erfolgen und somit gegen diesen Grundsatz verstoßen. Die Verarbeitung nach Treu und Glauben ist ein weit gefasster Begriff: Er verlangt, dass Forscher personenbezogene Daten nur in einer Weise verarbeiten, die andere vernünftigerweise erwarten würden, und dass sie nichts tun, was den betroffenen Personen schaden könnte.

Transparenz

Transparenz setzt voraus, dass Personen über die beabsichtigten Zwecke der Erhebung und Verwendung personenbezogener Daten, die rechtlichen Gründe für die Verarbeitung usw. in-

---

13 Europäischer Datenschutzbeauftragter, „A Preliminary Opinion on Data Protection and Scientific Research“, 23.

14 Datenschutz-Grundverordnung, Verordnung (EU) 2016/679, Erwägungsgrund 33.

15 Europäischer Datenschutzbeauftragter, „A Preliminary Opinion on Data Protection and Scientific Research“, 19.

formiert werden. Dies ist unabhängig davon erforderlich, ob personenbezogene Daten direkt von den betroffenen Personen erhoben werden (unabhängig davon, ob sie von der Person bewusst zur Verfügung gestellt oder durch Beobachtung der Person erhoben werden) oder ob sie aus einer anderen Quelle stammen (z. B. von Dritten, denen Daten anvertraut wurden, aus öffentlichen Quellen, von Datenmaklern oder von anderen Personen).16 Zu den mindestens bereitzustellenden Informationen gehören:17

- wer Ihr Unternehmen/Ihre Organisation ist (Ihre Kontaktdaten und die Kontaktdaten Ihres Datenschutzbeauftragten, falls zutreffend);
- warum Ihr Unternehmen/Ihre Organisation die personenbezogenen Daten nutzen wird (Zwecke);
- die Kategorien personenbezogener Daten, die verarbeitet werden;
- die Rechtsgrundlage für die Verarbeitung ihrer Daten;
- wie lange die Daten aufbewahrt werden;
- welche weiteren Empfänger die Daten erhalten könnten;
- ob die personenbezogenen Daten in ein Land außerhalb der EU übermittelt werden;
- dass sie das Recht auf eine Kopie der Daten (Auskunftsrecht) sowie weitere grundlegende Rechte im Bereich des Datenschutzes (siehe vollständige Liste der Rechte) haben;
- das Bestehen ihres Beschwerderechts bei einer Datenschutzbehörde;
- ihr Recht, die Einwilligung jederzeit zurückzuziehen;
- sofern zutreffend, das Bestehen einer automatisierten Entscheidungsfindung, nach welcher Logik die entsprechende Verarbeitung erfolgt und welche Auswirkungen sie hat.

Wenn Sie personenbezogene Daten aus einer anderen Quelle als den betroffenen Personen erhalten haben, müssen Sie diese innerhalb eines angemessenen Zeitraums, höchstens jedoch innerhalb eines Monats, nachdem Sie Zugang zu ihren personenbezogenen Daten erhalten haben, informieren.

Die Transparenzpflichten gelten nicht, wenn und soweit die betroffene Person bereits über die Informationen verfügt.18 Im Falle von personenbezogene Daten, die von Dritten erhoben wurden, gibt es drei weitere Situationen, in denen die Transparenzpflichten nicht gelten:19

- Wenn die Erteilung dieser Informationen sich als unmöglich erweist (dies gilt insbesondere für Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke);

---

16 Datenschutz-Grundverordnung, Verordnung (EU) 2016/679, Art. 12 Absätze 1, 5, 7, Art. 13, Art. 14, Erwägungsgründe 39, 58–62.

17 Europäische Kommission, „Welche Informationen müssen Personen, deren Daten erhoben werden, mitgeteilt werden?“.

18 Datenschutz-Grundverordnung, Verordnung (EU) 2016/679, Art. 13 Absatz 4, Art. 14 Absatz 5 Buchstabe a.

19 Datenschutz-Grundverordnung, Verordnung (EU) 2016/679, Art. 14 Absatz 5 Buchstabe b.

- Wenn die Erteilung dieser Informationen einen unverhältnismäßigen Aufwand erfordern würde (dies gilt insbesondere für Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke); oder
- Wenn die Bereitstellung der nach Artikel 14 Absatz 1 erforderlichen Informationen die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt.

Besondere Kategorien personenbezogener Daten / sensible Daten

Besondere Kategorien personenbezogener Daten bzw. sensible Daten20 sind Daten, aus denen die folgenden Merkmale einer betroffenen Person hervorgehen:

- rassische und ethnische Herkunft,
- politische Meinungen,
- religiöse oder weltanschauliche Überzeugungen,
- Gewerkschaftszugehörigkeit

oder bei denen es sich um:

- genetische Daten,
- biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person,
- Gesundheitsdaten oder
- Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person handelt.

Solche sensiblen Daten dürfen nicht erhoben werden, es sei denn, die Erhebung fällt unter eine der zehn in der DSGVO genannten Rechtsgrundlagen21, darunter die ausdrückliche Einwilligung, sowie wenn sie zu Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken mit den geeigneten Garantien erfolgt, die gemäß DSGVO gesetzlich vorgeschrieben und durch ein entsprechendes Gesetz vorgesehen sind.22 In Anbetracht der nationalen Unterschiede in den Gesetzen zur Regelung sensibler Daten, insbesondere genetischer, biometrischer oder gesundheitlicher Daten,23 sollten Forscher den Datenschutzbeauftragten ihrer Einrichtung oder ihre örtliche Datenschutzbehörde konsultieren, um mehr darüber zu erfahren, was zulässig ist und was nicht.

Auch wenn Daten im Zusammenhang mit strafrechtlichen Verurteilungen und Straftaten nach der DSGVO nicht als „sensibel“ eingestuft werden, verlangt die Verordnung, dass jede Verwen-

---

20 Datenschutz-Grundverordnung, Verordnung (EU) 2016/679, Art. 9 Absatz 1, Erwägungsgründe 51–56.

21 Datenschutz-Grundverordnung, Verordnung (EU) 2016/679, Art. 9 Absatz 2 Buchstabe a.

22 Datenschutz-Grundverordnung, Verordnung (EU) 2016/679, Art. 89.

23 Datenschutz-Grundverordnung, Verordnung (EU) 2016/679, Art. 9 Absatz 4.

dung solcher Daten durch Forscher zusätzlich durch ein EU- oder nationales Gesetz genehmigt werden muss und dass die in diesem Gesetz vorgesehenen Garantien eingehalten werden.24

2.2 Zweckbindung

Um den Grundsatz der Zweckbindung einzuhalten, sollten Forscher:

- den Zweck der Erhebung und Verwendung personenbezogener Daten klar und deutlich dokumentieren;
- Personen Informationen über die Zwecke der Erhebung und Verwendung ihrer Daten mitteilen;
- die Verarbeitung personenbezogener Daten auf die angegebenen Zwecke oder auf Zwecke beschränken, die mit den angegebenen Zwecken vereinbar sind;
- sicherstellen, dass die betroffenen Personen in den Fällen benachrichtigt werden, in denen der ursprüngliche Grund für die Verwendung der personenbezogenen Daten ein anderer war als die Einwilligung oder eine gesetzliche Vorschrift und diese Daten nun einer neuen, mit dem ursprünglichen Zweck vereinbaren Verwendung zugeführt werden. Dies sollte in angemessener Zeit vor der neuen Verwendung der personenbezogenen Daten erfolgen, damit die betroffene Person der Verarbeitung widersprechen kann;
- sicherstellen, dass sie in den Fällen, in denen der ursprüngliche Grund für die Verwendung der personenbezogenen Daten die Einwilligung war und diese Daten nun einer anderen Verwendung zugeführt werden, eine erneute Einwilligung einholen (unabhängig davon, ob es sich bei der neuen Verwendung um eine „vereinbare“ Verwendung handelt);
- sicherstellen, dass sie entweder eine Einwilligung oder eine eindeutige Pflicht/Funktion im öffentlichen Interesse haben, die in einem Gesetz vorgesehen ist, wenn sie die personenbezogenen Daten für andere als die angegebenen oder vereinbaren Zwecke verwenden wollen;
- sicherstellen, dass die neue Verwendung nach Treu und Glauben erfolgt sowie rechtmäßig und transparent ist.

Hintergrund

Der Zweck sollte „festgelegt, eindeutig und legitim“ sein.25 Die Artikel-29-Datenschutzgruppe stellt fest, dass „ein vager oder allgemeiner Zweck wie z. B. „künftige Forschung“ ohne nähere Angaben in der Regel nicht das Kriterium eines „festgelegten Zwecks“ erfüllt“. Allerdings hängt der Grad der Detailliertheit, mit dem ein Zweck angegeben werden sollte, von dem besonderen Kontext ab, in dem die Daten erhoben werden, sowie von den betroffenen personenbezogenen Daten. In einigen eindeutigen Fällen reicht eine einfache Formulierung aus, um einen angemes-

24 Datenschutz-Grundverordnung, Verordnung (EU) 2016/679, Art. 10.

25 Datenschutz-Grundverordnung, Verordnung (EU) 2016/679, Art. 5 Absatz 1 Buchstabe b.

sen festgelegten Zweck bereitzustellen, während in anderen Fällen mehr Details erforderlich sein können.“ 26

Die Erlaubnis zur Verarbeitung ist beschränkt auf:

- die rechtmäßigen Zwecke, die bei der Erhebung der Daten eindeutig festgelegt wurden, oder auf
- andere Zwecke, die mit den ursprünglichen Zwecken vereinbar sind

Die Vereinbarkeit kann anhand der folgenden Kriterien beurteilt werden:

a) der Zusammenhang zwischen den ursprünglichen Zwecken und den jeweiligen zusätzlichen Zwecken;
b) der Kontext, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich der Beziehung zwischen den betroffenen Personen und dem Verantwortlichen;
c) die Art der personenbezogenen Daten, insbesondere ob es sich um besondere Kategorien von (d. h. sensiblen) personenbezogenen Daten handelt oder ob personenbezogene Daten im Zusammenhang mit strafrechtlichen Verurteilungen und Straftaen verarbeitet werden;
d) die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen;
e) das Vorhandensein geeigneter Garantien, zu denen auch die Pseudonymisierung gehören kann.

Einige Zwecke, bei denen eine Vereinbarkeit *vermutet* wird, wenn geeignete, gesetzlich vorgeschriebene Garantieren getroffen werden, sind:

- im öffentlichen Interesse liegende Archivzwecke;
- wissenschaftliche oder historische Forschungszwecke; und
- statistische Zwecke.

Der EDSB stellt jedoch fest: „Die Vermutung ist keine allgemeine Erlaubnis, Daten in allen Fällen für historische, statistische oder wissenschaftliche Zwecke weiterzuverarbeiten. Jeder Fall muss unter Beachtung seiner eigenen Sachlage und Umstände betrachtet werden. Grundsätzlich können jedoch personenbezogene Daten, die beispielsweise im kommerziellen Kontext oder im Gesundheitswesen erhoben wurden, von dem ursprünglichen oder einem neuen Verantwortlichen für wissenschaftliche Forschungszwecke weiterverwendet werden, wenn geeignete Garantien vorhanden sind …Um die Achtung der Rechte der betroffenen Person zu gewährleisten, sollte die Vereinbarkeitsprüfung gemäß Artikel 6 Absatz 4 vor der Weiterverwendung von Daten für wissenschaftliche Forschungszwecke weiterhin in Betracht gezogen werden, insbesondere

26 Artikel-29-Datenschutzgruppe, Stellungnahme 03/2013 zur Zweckbindung, 15–16.

wenn die Daten ursprünglich für ganz andere Zwecke oder außerhalb des Bereichs der wissenschaftlichen Forschung erhoben wurden.“27

2.3 Datenminimierung

Um dem Grundsatz der Datenminimierung gerecht zu werden, müssen/dürfen Forscher:

- sicherstellen, dass sie nur dann personenbezogene Daten erheben, wenn diese angemessen, erheblich und für den festgelegten Zweck erforderlich sind;
- keine größeren Mengen personenbezogener Daten als erforderlich erheben;
- keine detaillierteren oder granulareren Arten personenbezogener Daten erheben als erforderlich;
- sicherstellen, dass sie personenbezogene Daten nicht länger als erforderlich speichern;
- die gespeicherten personenbezogenen Daten regelmäßig überprüfen, um festzustellen, ob sie die oben genannten Anforderungen weiterhin erfüllen, und alle personenbezogenen Daten löschen, die nicht den Anforderungen entsprechen.

Hintergrund

Angemessenheit, Erheblichkeit und Erforderlichkeit sind drei Voraussetzungen für die Verarbeitung personenbezogener Daten gemäß der DSGVO. So dürfen Daten, die unangemessen, d. h. für den angegebenen Zweck ungeeignet sind, nicht erhoben oder verarbeitet werden. Sie müssen auch erheblich sein, d. h. dem angegebenen Zweck dienen. Und die Einschränkung der Erforderlichkeit hat drei Aspekte:

- Menge der Daten;
- Granularität der Daten; und
- Dauer der Speicherung (ausführlicher unter dem Grundsatz der „Speicherbegrenzung“ weiter unten erläutert).

Vereinfacht ausgedrückt sollten Forscher also versuchen, so wenig personenbezogene Daten wie erforderlich zu erheben, zu speichern und zu verarbeiten, und zwar für einen so kurzen Zeitraum wie möglich, um den festgelegten Zweck zu erfüllen. Dies wird, wie auch bei anderen Grundsätzen, sowohl durch technische als auch durch organisatorische Maßnahmen erreicht.

Die Datenminimierung wird in der DSGVO als besonders zu beachtender Punkt für diejenigen aufgeführt, die personenbezogene Daten für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke verarbeiten, da diese unter eine etwas gelockerte Regelung fallen, wenn es um den Grundsatz der Zweckbindung geht. Zu den Maßnahmen, die zur Datenminimierung ergriffen werden können, gehört die Pseudonymisierung, sofern dies machbar ist.

---

27 Europäischer Datenschutzbeauftragter, „A Preliminary Opinion on Data Protection and Scientific Research“, 22–23.

2.4 Richtigkeit

Um den Grundsatz der Richtigkeit zu erfüllen, sollten Forscher:

- sicherstellen, dass die von ihnen aufbewahrten personenbezogenen Daten sachlich richtig sind;
- sicherstellen, dass die von ihnen aufbewahrten personenbezogenen Daten auf dem neuesten Stand sind;
- Prozesse einrichten, um die Richtigkeit der Daten zu überprüfen, mit Zeitvorgaben für die Überprüfung der Richtigkeit;
- alle sachlich unrichtigen oder irreführenden bei Entdecken sofort berichtigen;
- alle Fehler aufzeichnen, die als Fehler bewahrt werden müssen, und die Gründe für die Aufbewahrung angeben;
- allen Anträgen auf Berichtigung seitens Personen nachkommen.

Hintergrund

Der Grundsatz der Richtigkeit umfasst zwei Aspekte: sachliche Richtigkeit und Daten auf dem neuesten Stand. Es ist untersagt, unrichtige personenbezogene Daten zu verwenden, da diese für den Zweck, für den die Daten erhoben werden, ungeeignet sein könnten. Außerdem könnten unrichtige Daten den betroffenen Personen schaden und somit gegen den Grundsatz der Verarbeitung nach Treu und Glauben verstoßen. Daher sind Forscher verpflichtet, unrichtige personenbezogene Daten zu löschen oder zu berichtigen.

Um die Richtigkeit der personenbezogenen Daten sicherzustellen, haben die betroffenen Personen das Recht, die Berichtigung sie betreffender Daten zu verlangen.

2.5 Speicherbegrenzung

Um die Einhaltung des Grundsatzes der Speicherbegrenzung zu gewährleisten, müssen Forscher:

- sicherstellen, dass sie personenbezogene Daten nicht länger speichern, als es für den Zweck, für den sie erhoben wurden, erforderlich ist;
- sicherstellen, dass nicht mehr benötigte personenbezogene Daten entweder gelöscht oder anonymisiert werden;
- den Zweck dokumentieren, für den die personenbezogenen Daten erhoben wurden, und wie lange die Daten zur Erreichung dieses Zwecks aufbewahrt werden müssen;
- den Grund für die Dauer der Speicherung dokumentieren;
- die Notwendigkeit der Aufbewahrung überprüfen, wenn die festgelegte Speicherfrist abgelaufen ist;
- die im öffentlichen Interesse liegenden Archivzwecke, wissenschaftlichen oder historischen Forschungszwecke oder statistischen Zwecke ermitteln und dokumentieren, für die die Daten länger als unbedingt erforderlich gespeichert werden, falls die Daten im

Rahmen der Ausnahmeregelung für solche Forschungen gespeichert werden, zusammen mit der Einhaltung der gesetzlich laut Art. 89 festgelegten angemessenen Garantien.

Hintergrund

Forscher sollten personenbezogene Daten nicht länger aufbewahren, als es für die angegebenen Zwecke, für die die Daten erhoben wurden, erforderlich ist. Die Daten sollten vernichtet werden, sobald sie für die angegebenen Zwecke nicht mehr erforderlich sind.

Eine Möglichkeit, dies zu erreichen, ist die Anonymisierung von Daten, wo immer dies möglich ist, sodass personenbezogene Daten in Daten umgewandelt werden, die eine direkte oder indirekte Identifizierung der betroffenen Personen, auf die sie sich beziehen, nicht mehr ermöglichen.

Forscher dürfen personenbezogene Daten länger als unbedingt erforderlich aufbewahren, wenn die personenbezogenen Daten ausschließlich zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken verwendet werden sollen und wenn sie darüber hinaus die in Artikel 89 DSGVO festgelegten Bedingungen erfüllen, d. h. über angemessene Garantien in Form von geeigneten technischen und organisatorischen Maßnahmen zum Schutz der Rechte der betroffenen Person verfügen. Darüber hinaus sollten Forscher sicherstellen, dass sie solche personenbezogenen Daten nicht als Grundlage für Maßnahmen oder Entscheidungen in Bezug auf eine bestimmte Person verwenden.28

2.6 Integrität und Vertraulichkeit

Um den Grundsatz der Integrität und Vertraulichkeit einzuhalten, müssen die Forscher:

- sicherstellen, dass personenbezogene Daten sicher aufbewahrt werden, indem sie vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen geschützt werden;
- die technischen und organisatorischen Maßnahmen dokumentieren, die zur Gewährleistung der Sicherheit getroffen wurden.

Hintergrund

Forscher sind verpflichtet, personenbezogene Daten sicher aufzubewahren, d. h. die Vertraulichkeit, Integrität und Verfügbarkeit der Daten zu gewährleisten und sie so vvor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung zu schützen, und zwar sowohl durch geeignete technische als auch organisatorische Maßnahmen.

28 Artikel-29-Datenschutzgruppe, Stellungnahme 03/2013 zur Zweckbindung, 28.

Die Datensicherheit ist somit ein zentraler Bestandteil des Schutzes personenbezogener Daten. Bei der Prüfung der Frage, ob Vertraulichkeit und Integrität erfüllt sind, ist es wichtig, dies aus der Sicht der betroffenen Personen und nicht aus der Sicht der Forscher zu betrachten. Anders ausgedrückt: Selbst wenn den Forschern durch die unbefugte Verarbeitung kein Schaden entstanden ist, heißt das nicht, dass die unbefugte Verarbeitung keinen Schaden verursacht hat.

Forscher müssen somit klar festgelegte Rollen und Verantwortlichkeiten haben, damit klar ist, wer für ein bestimmtes Forschungsvorhaben Zugang zu personenbezogenen Daten hat.

2.7 Rechenschaftspflicht

Um den Grundsatz der Rechenschaftspflicht einzuhalten, müssen die Forscher:

- sicherstellen, dass sie das Datenschutzrecht proaktiv und organisiert einhalten;
- sich über die ihnen auferlegten Pflichten und die Rechte, die betroffene Personen nach dem Gesetz haben, informieren;
- klare Richtlinien, Verfahren und technische Maßnahmen einführen, die die Einhaltung der oben genannten Grundsätze und des Gesetzes gewährleisten;
- sicherstellen, dass der Ansatz „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“ befolgt wird;
- sicherstellen, dass ihre Organisation über einen Datenschutzbeauftragten verfügt, wenn es sich um eine öffentliche Behörde oder Einrichtung handelt, wenn sie regelmäßig und systematisch mit Personen in großem Umfang interagieren oder wenn sie in großem Umfang besondere Datenkategorien wie z. B. sensible Daten verarbeiten;
- eine Datenschutz-Folgenabschätzung durchführen, wenn die Art der gewünschten Datenverarbeitung voraussichtlich ein hohes Risiko zur Folge hat. Dies gilt insbesondere dann, wenn die Forscher planen, systematisch und umfassend Profile mit erheblichen Auswirkungen zu erstellen, Daten besonderer Kategorien oder strafrechtlich relevante Daten in großem Umfang zu verarbeiten oder öffentlich zugänglicher Bereiche systematisch und in großem Umfang zu überwachen;
- Personen in der Regel über den Datenschutzbeauftragten ihrer Einrichtung, spätestens innerhalb von 72 Stunden über eine Datenschutzverletzung zu informieren, wenn die Verletzung voraussichtlich zu einem Risiko für die Rechte und Freiheiten der Personen führt, deren personenbezogene Daten verletzt wurden;
- unverzüglich den Anträgen betroffener Person auf Ausübung der ihnen zustehenden Rechte entsprechen;
- die Einhaltung aller oben genannten Grundsätze und der gesetzlichen Bestimmungen dokumentieren.

Hintergrund

Personen, die personenbezogene Daten erheben und verwenden, wie z. B. Forscher, sind für die Einhaltung der oben genannten Grundsätze verantwortlich. Insbesondere müssen sie nachweisen können, dass sie die Grundsätze einhalten.

Daher muss die Einhaltung dieser Grundsätze geplant und dokumentiert werden. Beispielsweise sollten Forscher in der Lage sein, zu begründen, warum sie bestimmte personenbezogene Daten mit der jeweils erhobenen Granularität benötigen und wie lange die Daten gespeichert werden. Bei vielen Aspekten der Rechenschaftspflicht wäre es von Vorteil, automatisierte technische Maßnahmen anzuwenden.

3 Bewährte Praktiken in Bezug auf die Datenschutzgrundsätze

Bewährte Praktiken im Zusammenhang mit den Datenschutzgrundsätzen umfassen Praktiken, die über das in der DSGVO und den nationalen Gesetzen vorgeschriebene Minimum hinausgehen. Obwohl sie nicht gesetzlich vorgeschrieben sind, erleichtern sie den Forschern die Einhaltung der in diesem Dokument bereits erörterten Datenschutzgrundsätze.

3.1 Anonymisierung, Pseudonymisierung und Verschlüsselung

Die verschiedenen Anforderungen der DSGVO gelten nicht, wenn Forscher keine *personenbezogenen Daten* verarbeiten. Daher sollten sie nach Möglichkeit immer prüfen, ob die für die Forschung benötigten Daten die Identifizierung einer Person ermöglichen. Zu beachten ist jedoch, dass die DSGVO zwischen pseudonymisierten und anonymisierten Daten unterscheidet. Das bloße Entfernen aller persönlichen Kennungen führt nicht automatisch zu einer „Anonymisierung" der Daten.

Pseudonymisierte personenbezogene Daten sind personenbezogene Daten, die ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können; mit zusätzlichen Informationen kann die betroffene Person jedoch identifiziert werden.

Anonymisierten Daten müssen nicht nur verhindern, eine bestimmte Person auf der Grundlage der erhobenen und verarbeiteten Daten zu identifizieren, sondern es müssen auch alle Mittel berücksichtigt werden, die von anderen „nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern". Bei der Feststellung, welche Mittel „nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden", so die DSGVO, „sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind."29 Wenn eine Deanonymisierung der Daten somit praktisch möglich ist, dann können diese nicht als anonymisierte Daten betrachtet werden – es wären dann pseudonymisierte Daten, die immer noch als personenbezogene Daten gelten.

Die DSGVO schlägt die Pseudonymisierung und Verschlüsselung als zwei Mittel zur Gewährleistung einer besseren Sicherheit personenbezogener Daten vor. Beide Techniken würden dazu beitragen, die Anforderungen des Grundsatzes der Integrität und Vertraulichkeit zu erfüllen. Die Pseudonymisierung würde zudem dazu beitragen, den Grundsatz der Datenminimierung einzuhalten. Bei einigen Arten der Datenverarbeitung zu wissenschaftlichen Forschungszwecken, bei

29 Datenschutz-Grundverordnung, Verordnung (EU) 2016/679, Erwägungsgrund 26.

denen der Grundsatz der Zweckbindung etwas gelockert ist, verlangt die DSGVO, dass Forscher nach Möglichkeit die Daten minimieren sollten, und zwar durch Pseudonymisierung oder auch durch Anonymisierung, wenn dies machbar ist.30

3.2 Aggregierte und grobe Daten

Ziehen Sie aggregierte Daten nach Möglichkeit Daten auf individueller Ebene vor sowie grobe Daten granularen Daten vor. Wenn beispielsweise Altersdaten erforderlich sind, sollten Sie diese in Form einer Zahl und nicht als Geburtsdatum erfassen. Noch besser ist es, eine Altersspanne anstelle eines genauen Alters zu erfassen, sofern diese ausreicht. Wenn schließlich die Daten mehrerer Personen aggregiert und die Daten auf individueller Ebene vernichtet werden können, sollten Sie dies tun.

3.3 Transparenz

Wenn personenbezogene Daten im Internet erfasst werden, sollten Sie einen klar erkennbaren Link zu den Datenschutzerklärungen bzw. -hinweisen bereitstellen. Alternativ kann die Bereitstellung der Informationen auch auf der gleichen Seite erfolgen, auf der die personenbezogenen Daten erhoben werden.31 Wenn sich die Art und Weise, wie Sie personenbezogene Daten verarbeiten, ändert, sollten der betroffenen Person alle Informationen erneut zur Verfügung gestellt werden, wobei mühelos erkennbar sein sollte, welche Informationen neu sind.32

3.4 Mehrere Rechtsgrundlagen für die Verarbeitung

Die DSGVO scheint die Möglichkeit zuzulassen, dass mehrere Rechtsgrundlagen für die Verarbeitung derselben personenbezogenen Daten herangezogen werden. Dies könnte jedoch zu einer Situation führen, in der zwei Rechtsgrundlagen (z. B. Einwilligung und berechtigtes Interesse) verwendet wurden, von denen eine wegfällt (z. B. wenn eine Person ihre Einwilligung widerruft). In einem solchen Fall ist es unklar, was das Gesetz vorschreibt, und es gibt keine eindeutige einhellige Meinung der verschiedenen Rechtsinstanzen. Diese Unsicherheit sollte vorzugsweise durch ein konservatives Verständnis des Gesetzes gelöst und die Verarbeitung der Daten eingestellt werden, wenn eine der Rechtsgrundlagen wegfällt. Um diese Situation zu vermeiden, ist es unter Umständen besser, die Einwilligung nicht mit anderen Rechtsgrundlagen zu kombinieren. In solchen Fällen kann es besser sein, die Verarbeitung von Daten auf den am besten geeigneten Grund zu beschränken.

3.5 Einwilligung im Datenschutz und in der Ethik

Die Einwilligung als Rechtsgrundlage für die Verarbeitung von Daten nach dem Datenschutzrecht unterscheidet sich von der „Einwilligung nach Aufklärung“ als Grundsatz der Ethik für die

---

30 Datenschutz-Grundverordnung, Verordnung (EU) 2016/679, Art. 89 Absatz 1.

31 Artikel 29-Datenschutzgruppe, Leitlinien für Transparenz gemäß der Verordnung 2016/679, 8.

32 Artikel 29-Datenschutzgruppe, 27–28.

Forschung am Menschen33 Daher ist es immer besser, getrennte Einwilligungsformulare bereitzustellen und jede Art von Einwilligung separat einzuholen. Selbst wenn die Einrichtung beide Einwilligungserklärungen mit einem einzigen Formular einholt, sollte klar festgehalten werden, wozu jeder Teilnehmer im Hinblick auf die Forschung eingewilligt hat.

Selbst in Fällen, in denen die Einwilligung nicht als Rechtsgrundlagen im Rahmen der DSGVO verwendet wird, „könnte die *Einwilligung nach Aufklärung* als Teilnehmer an einer Forschung am Menschen immer noch als ein „angemessener Schutz" der Rechte der betroffenen Person dienen."34

3.6 Zulässigkeit, Treu und Glauben und ethische Zulassungen

Die Zulässigkeit der Datenerhebung wird manchmal durch Gesetze bestimmt, die ethische Anforderungen vorschreiben (z. B. für klinische Versuche). Aber selbst wenn für bestimmte Forschungen keine gesetzlichen Anforderungen an die ethische Freigabe gelten, sollte man am besten von der Annahme ausgehen, dass eine unethische Datenerhebung oder -verwendung auch als unzulässiger Zweck im Sinne der DSGVO angesehen wird und dem Grundsatz der Verarbeitung nach Treu und Glauben nicht entspricht. So sollten Forscher beispielsweise von einer Datenverarbeitung absehen, die von einer Ethikkommission missbilligt wird.

3.7 Datenschutzbehörden und Ethikkommissionen

In Anbetracht der zunehmenden Verflechtung zwischen ethischen Fragen und Fragen des Schutzes der Privatsphäre und des Datenschutzes wäre es für die Ethikkommissionen von Vorteil, wenn sie sich stärker mit den Datenschutzbeauftragten und -behörden abstimmen würden.35 Es gibt viele Fälle (beispielsweise genetische Daten), in denen die Verwendung der personenbezogenen Daten einer Person in der Forschung nicht nur diese Person selbst, sondern auch andere betreffen würde. Der Rahmen des Datenschutzes allein reicht möglicherweise nicht aus, um diese Bedenken in einer Weise zu erfassen, wie es ein kombinierter Rahmen aus Forschungsethik und Datenschutz könnte. Dies erfordert eine stärkere Zusammenarbeit zwischen denjenigen, die sich mit ethischen Fragen befassen, und denjenigen, die Datenschutzfragen behandeln.

3.8 Datenschutzrichtlinien und Datenschutzbeauftragte

Viele Forschungseinrichtungen haben neben ethischen Richtlinien auch Datenschutzrichtlinien erlassen. Forscher sollten sich mit den Richtlinien ihrer Einrichtung vertraut machen. In vielen Fällen haben auch die Geldgeber besondere Anforderungen in Bezug auf den Datenschutz. Bei allen unter Horizont 2020 finanzierten Projekten ist beispielsweise die Einbindung eines Datenschutzbeauftragten (DSB) erforderlich, sofern ein solcher ernannt wurde, wobei auch in den

---

33 Europäischer Datenschutzbeauftragter, „A Preliminary Opinion on Data Protection and Scientific Research", 19–20.

34 Europäischer Datenschutzbeauftragter, 20.

35 Europäischer Datenschutzbeauftragter, 25.

Fällen, in denen ein DSB nicht gesetzlich vorgeschrieben ist,36 eine Datenschutzrichtlinie ausgearbeitet werden muss.

Es gibt einige Fragen, für die nicht nur die DSGVO, sondern auch die Gesetze der Mitgliedsstaaten gelten. Wichtig für Forscher ist, dass die besondere Datenschutzregelung in Bezug auf die Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken Lockerungen der Rechte betroffener Personen und der sich daraus ergebenden Pflichten des Forschers vorsehen kann, wenn die nationalen Rechtsvorschriften dies zulassen. Für die Verarbeitung personenbezogener Daten zu einem dieser Zwecke sind geeignete Garantien erforderlich. Die Forscher müssen sich an die oben genannten Grundsätze halten und insbesondere auf technische und organisatorische Maßnahmen achten, mit denen die Datenminimierung gewährleistet wird.37 Da die gesetzlichen Pflichten der Forscher nicht einheitlich sind, sollten sie nach Möglichkeit den Datenschutzbeauftragten und die Datenschutzrichtlinien ihrer Einrichtung konsultieren, da diese ihnen bei der Festlegung der geltenden gesetzlichen und außergesetzlichen Normen behilflich sein können.

3.9 Datenschutz-Folgenabschätzung

Wenn ein Projekt mit einer großen Menge personenbezogener Daten oder mit personenbezogenen Daten schutzbedürftiger Personen zu tun hat, wäre es von Vorteil, ein solches Projekt mit dem DSB zu besprechen und eine Datenschutz-Folgenabschätzung (DPIA) durchzuführen, auch wenn dies nicht gesetzlich vorgeschrieben ist. Der EDSB stellt fest, dass eine „Datenschutz-Folgenabschätzung für Datenverarbeitungsvorgänge, die ein hohes Risiko für die betroffenen Personen darstellen, zwingend erforderlich ist, beispielsweise wenn zwei der folgenden Kriterien zutreffen":38 1. Systematische Bewertung/Profiling 2. Automatisierte Entscheidungsfindung 3. Systematische Überwachung: 4. Verarbeitung sensibler Daten 5. Umfangreiche Datenverarbeitung 6. Abgleich/Kombination von Datenmengen mit unterschiedlichen Zwecken 7. Daten schutzbedürftiger betroffener Personen 8. Neuartige Technologien 9. Hinderung betroffener Personen an der Rechtsausübung, Inanspruchnahme von Dienstleistungen bzw. Vertragsdurchführung

36 Datenschutz-Grundverordnung, Verordnung (EU) 2016/679, Art. 38.

37 Datenschutz-Grundverordnung, Verordnung (EU) 2016/679, Art. 89.

38 Europäischer Datenschutzbeauftragter, Entscheidung des Europäischen Datenschutzbeauftragten vom 16. Juli 2019 über gemäß Artikel 39 Absätze 4 und 5 der Verordnung (EU) 2018/1725 erstellte DSFA-Listen, Anhang 1.

4 Anhänge

4.1 Anhang 1: Wichtige Ressourcen

Das PANELFIT-Projekt hat detaillierte Leitlinien zu datenschutzrechtlichen, ethischen und rechtlichen Fragen in der IKT-Forschung und -Innovation sowie eine kritische Analyse des Rechtsrahmens für den IKT-Datenschutz erstellt. Der CCDP stützt sich weitgehend auf diese beiden Dokumente. Diejenigen, die mehr über die im CCDP aufgeworfenen Fragen erfahren oder die Aspekte des Datenschutzes verstehen möchten, die im CCDP nicht behandelt wurden, sollten diese Leitlinien konsultieren, die weitaus mehr Einzelheiten enthalten.

Beide Dokumente finden Sie unter: https://www.panelfit.eu/deliverables/.

Nachstehend werden einige weitere wichtige Ressourcen für Forscher aufgeführt, die mehr über Datenschutz und verantwortungsvolle Forschung und Innovation erfahren möchten.

- Europäischer Datenschutzbeauftragter. „A Preliminary Opinion on Data Protection and Scientific Research“, Januar 2020. https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf.
- Artikel 29-Datenschutzgruppe. „Stellungnahme 03/2013 zur Zweckbindung“, 2. April 2013. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.
- Artikel 29-Datenschutzgruppe. „Stellungnahme 5/2014 zu Anonymisierungstechniken“, 10. April 2014. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf *.
- Artikel 29-Datenschutzgruppe. „Leitlinien für Transparenz gemäß der Verordnung 2016/679“, 29. November 2017. https://www.datenschutzstelle.li/application/files/3615/3674/7263/wp259rev01_de.pdf .
- Europäischer Datenschutzausschuss. „Leitlinien 3/2020 für die Verarbeitung von Gesundheitsdaten für wissenschaftliche Forschungszwecke im Zusammenhang mit dem COVID-19-Ausbruch.“ Leitlinien, 30. April 2020. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_de.pdf.
- Europäischer Datenschutzausschuss. „Leitlinien 4/2019 zu Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen.“ Leitlinien, 13. November 2019. https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf.

- Europäischer Datenschutzausschuss. „Leitlinien 4/2019 zu Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen.“ Leitlinien, 20. Oktober 2020. https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_de.pdf.

- Europäischer Datenschutzbeauftragter. „Leitlinien des EDSB für die Bewertung der Verhältnismäßigkeit, die die Grundrechte auf Privatsphäre und den Schutz personenbezogener Daten einschränken“, 19. Dezember 2019. https://edps.europa.eu/sites/default/files/publication/19-12-19_edps_proportionality_guidelines2_de.pdf.

- Europäischer Datenschutzbeauftragter. „Flowcharts and Checklists on Data Protection.“ 2020. https://doi.org/10.2804/823679.

- Europäische Kommission (Generaldirektion Forschung und Innovation). „Ethics and Data Protection“, November 2018. https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf.

- ALLEA. *Europäischer Verhaltenskodex für Integrität in der Forschung*. 2. Fassung, 2017. https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/h2020-ethics_code-of-conduct_en.pdf.

- Projekt RESPECT „RESPECT Code of Practice for Socio-Economic Research.“ Institute for Employment Studies, 2004. http://www.respectproject.org/code/respect_code.pdf

- EFAMRO und ESOMAR. „Guidance Note for the Research Sector:Appropriate Use of Different Legal Bases under the GDPR.“ Juni 2017. https://www.esomar.org/uploads/public/government-affairs/position-papers/EFAMRO-ESOMAR_GDPR-Guidance-Note_Legal-Choice.pdf.

- Wilford, Sara, Malcolm Fisk und Bernd Stahl. „Guidelines for Responsible Research and Innovation.“ Projekt GREAT, 2016. https://www.great-project.eu/Deliverables10.

- Der Europäische Datenschutzausschuss hat erklärt, dass er „beabsichtigt, Leitlinien zu den „horizontalen und komplexen“ Bedingungen für die Anwendbarkeit der „Vermutung der Vereinbarkeit“ auf die Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke herauszugeben, wie dies in Artikel 5 Absatz 1 Buchstabe b DSGVO vorgesehen ist.“39 Das wird bei Herausgabe für die Forscher nützlich sein.

39 Europäischer Datenschutzausschuss, „Stellungnahme des Ausschusses (Artikel 70 Absatz I Buchstabe b)“.

4.2 Anhang 2: Literaturverzeichnis

Artikel 29-Datenschutzgruppe. „Leitlinien für Transparenz gemäß der Verordnung 2016/679“, 29. November 2017. https://www.datenschutzstelle.li/application/files/3615/3674/7263/wp259rev01_de.pdf.

———.„Stellungnahme 03/2013 zur Zweckbindung“, 2. April 2013. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

Europäische Kommission. „Wissenschaft mit der und für die Gesellschaft.” Horizon 2020, 11. November 11 2013. https://ec.europa.eu/programmes/horizon2020/en/h2020-section/science-and-society.

———.„Welche Informationen müssen Personen, deren Daten erhoben werden, mitgeteilt werden?“ Text. Grundsätze der Datenschutz-Grundverordnung: Welche Informationen müssen Personen, deren Daten erhoben werden, mitgeteilt werden?, 8. Januar 2018. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/what-information-must-be-given-individuals-whose-data-collected_de.

Europäischer Datenschutzausschuss. „Stellungnahme des Ausschusses (Artikel 70 Absatz I Buchstabe b)“. Stellungnahme, 23. 2019. https://edpb.europa.eu/sites/default/files/files/file1/edpb_opinionctrq_a_final_de.pdf.

Europäischer Datenschutzbeauftragter. „A Preliminary Opinion on Data Protection and Scientific Research“, Januar 2020. https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf.

———. „Entscheidung des Europäischen Datenschutzbeauftragten vom 16. Juli 2019 über gemäß Artikel 39 Absätze 4 und 5 der Verordnung (EU) 2018/1725 erstellte DSFA-Listen“, 16. Juli 2019. https://edps.europa.eu/sites/default/files/publication/19-07-16_edps_dpia_list_en.pdf.

Datenschutz-Grundverordnung, Verordnung (EU) 2016/679 (2016). https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A02016R0679-20160504.

„Erklärung von Rom über verantwortungsvolle Forschung und Innovation in Europa“, 21. November 2014. https://ec.europa.eu/research/swafs/pdf/rome_declaration_RRI_final_21_November.pdf.

4.3 Anhang 3: Verfahren zur Erstellung eines Verhaltenskodex zum Datenschutz für verantwortungsvolle Forschung und Innovation

Unser Ziel war es, eine Vielzahl von Stakeholdern in die Überarbeitung des CCDP einzubeziehen und so viel Feedback wie möglich zu erhalten. Der Konsultationsprozess wird im Folgenden beschrieben.

Der erste Entwurf des CCDP wurde im Oktober 2020 in Umlauf gebracht und die endgültige Version dann im August 2021 konsolidiert. In den verschiedenen Phasen des Prozesses wurden fünf Versionen erstellt, wobei das Feedback in jedem Schritt berücksichtigt wurde. Die nachstehenden Abschnitte fassen den CCDP-Feedbackprozess zusammen, einschließlich der wichtigsten eingegangenen Kommentare sowie der jeweils unternommenen Schritte zur Beantwortung.

Der Umfang der einzelnen Feedback-Phasen wird im Folgenden beschrieben:

• Konsultation interner Experten (PANELFIT): Die erste, im Oktober 2020 erstellte Version des CCDP wurde vom PANELFIT-Projektkonsortium geprüft, dem unter anderem Experten für Cybersicherheit, Governance, Privatsphäre und Datenschutz angehören.

• Konsultation externer Experten (Stakeholder): Diese Konsultation wurde im Rahmen des vom Projekt organisierten „Mutual Learning Encounter“ für Stakeholder durchgeführt. An dieser Online-Veranstaltung, die am 20. April 2021 stattfand, nahmen 13 Personen der folgenden Organisationen teil: ALLEA, Europäische Gruppe für Ethik der Naturwissenschaften und der Neuen Technologien (EGE) der Europäischen Kommission, Universität Vilnius, NEC Laboratories Europe, Tech Uni Cluj-Napoca, Museum für Naturkunde, COCIR, Universität Babes-Bolyai, Research Centre for Data Science and Senior Lecturer, School of Computing, Electronics and Mathematics an der Universität von Coventry, Uni Babes Bolyai, Europäische Kommission, Open Science (DG RTD), Universität von Tilburg, School of Computing, Electronics and Mathematics an der Universität von Coventry, Universität Kopenhagen.

• Konsultation externer Forscher: Forscher aus verschiedenen Disziplinen nahmen an dem vom Projekt organisierten Mutual Learning Encounter für Forscher teil. Die Online-Veranstaltung fand am 24. Juni 2021 statt.

• Öffentliche Konsultation: Der CCDP wurde auf der PANELFIT-Webseite veröffentlicht, zusammen mit einem Formular, um Feedback von allen interessierten Personen zu erhalten. Die Teilnahme am Feedback wurde über soziale Netzwerke und Mailinglisten gefördert. Das Dokument war von März bis August 2021 unter folgendem Link verfügbar: https://www.panelfit.eu/a-code-of-conduct-on-data-protection-for-responsible-research-and-innovation-ccdp/

• Befragung von Forschern: Die Umfrage war Teil des CCDP-Feedback-Abschlussprozesses. Sie wurde vor, während und nach der MLE für Forscher durchgeführt. Das Feedback trug zur Verbesserung des Abschnitts über bewährte Praktiken bei.