



Nachbericht zur Veranstaltung „Citizen Science & Recht“

Inhaltsverzeichnis

1	RECHTLICHER RAHMEN: DIE DATENSCHUTZGRUNDVERORDNUNG	1
1.1	PERSONENBEZOGENE DATEN.....	1
1.2	ROLLENVERTEILUNG (ART 4 DSGVO).....	2
1.3	RECHTE DER BETROFFENEN PERSONEN.....	3
1.4	BESONDERHEITEN BEIM RECHT AUF LÖSCHUNG UND WIDERRUFSRECHT	3
1.5	GRUNDSATZ DER DATENMINIMIERUNG UND SPEICHERBEGRENZUNG	4
1.6	RECHTMÄßIGKEIT DER VERARBEITUNG	4
1.7	ÖFFNUNGSKLAUSELN UND FORSCHUNGSORGANISATIONSGESETZ (ART 89 DSGVO)	5
2	PRAKTISCHE UMSETZUNG IN 8 SCHRITTEN.....	5
3	WEITERE ANFORDERUNGEN	8

Citizen Science & Recht

Am 27. Juni 2018 fand die Veranstaltung „Citizen Science & Recht“ statt, die vom Citizen Science Network Austria, der Universität Wien, dem Zentrum für Citizen Science und dem Bundesministerium für Bildung, Wissenschaft und Forschung organisiert wurde. Ziel der gemeinsamen Veranstaltung war es, jene Bereiche aufzuzeigen, auf die Projektleiterinnen und Projektleiter bei der Umsetzung der Datenschutzgrundverordnung im Besonderen achten sollten.

Die Vortragende, Dipl.-Ing. Annemarie Hofer, ist Mitglied der Arbeitsgruppe für juristische Aspekte in Citizen Science bei der Plattform Österreich forscht und ist seit Mai 2018 bei der [denkstatt GmbH](#) im Bereich Legal Compliance tätig. Zuvor war sie am Institut für Rechtswissenschaften an der Universität für Bodenkultur tätig. Im Rahmen ihrer Masterarbeit hat sie sich mit datenschutzrechtlichen Aspekten bei Citizen Science auseinandergesetzt.

In ihrem Vortrag stellte sie die Ergebnisse ihrer Masterarbeit vor und führte zuerst theoretisch in die Datenschutzgrundverordnung ein, klärte Begrifflichkeiten und zeigte die wichtigsten Neuerungen auf. Im Anschluss ging sie auf die praktische Umsetzung ein und erklärte diese anhand von acht Schritten, an denen sich Citizen Science-Projekte orientieren können.

Folgende Zusammenfassung dient als Nachlese zur gut besuchten Veranstaltung im Palais Harrach in Wien.

1 Rechtlicher Rahmen: Die Datenschutzgrundverordnung

Die Datenschutzgrundverordnung (DSGVO) ist seit 25. Mai 2018 in Kraft und legt die rechtmäßige Verarbeitung aller personenbezogenen Daten, das heißt, wann personenbezogene Daten verarbeitet werden dürfen, fest. Für spezielle Anwendungsbereiche existieren in Österreich weitere Regelungen zum Datenschutz. Für die wissenschaftliche Forschung ist das z.B. Forschungsorganisationsgesetz (FOG) (siehe Punkt 1.7).

1.1 Personenbezogene Daten

Der Begriff „personenbezogene Daten“ bezieht sich auf all jene Informationen, die dazu führen, dass eine natürliche Person identifiziert bzw. erkannt werden kann. Das heißt, einzelne Daten zu natürlichen Personen alleine müssen nicht unbedingt personenbezogene Daten sein. Hier sind der Kontext und die Kombination der Daten relevant, durch die eine Person konkret identifizierbar werden würde.

Beispiel: Die Angaben zu einer Person, wie z.B. ‚männlich‘ und ‚über 80 Jahre‘, lassen in einer Großstadt keinen Rückschluss auf eine bestimmte Person zu, sind also nicht personenbezogen. Diese Angaben können aber zu personenbezogenen Daten werden, wenn der Personenkreis so klein ist, dass die Person dennoch eindeutig identifiziert werden kann,

z.B. in einem kleinen Dorf. So sind auch E-Mail-Adressen, die keinen Rückschluss auf Personen geben, nicht als personenbezogene Daten einzustufen. Eine Anonymisierung wird dennoch empfohlen um Missbrauch vorzubeugen.

Eine spezielle Form der personenbezogenen Daten sind die besonderen Kategorien personenbezogener Daten, früher „sensible Daten“ genannt. Hier muss man bei der Speicherung besonders achtsam vorgehen und benötigt eine ausdrückliche Einwilligung der betroffenen Personen. Hierzu zählen etwa rassische und ethnische Herkunft, Gesundheitsdaten, sexuelle Orientierung, uvm.

Mit der DSGVO wurden zudem neue Begrifflichkeiten für Daten eingeführt. Man unterscheidet etwa zwischen pseudonymen und anonymen Datensätzen.

Bei pseudonymen Daten kann der Personenbezug mittels zusätzlicher Information durch berechnete Personen (wieder) hergestellt werden. Beispiele hierfür sind etwa Matrikelnummern oder andere Zuordnungslisten. Diese Daten unterliegen der DSGVO.

Bei anonymen Daten kann der Personenbezug nicht (mehr) hergestellt werden. Die Anonymisierung ist auch nicht reversibel, weshalb diese Daten nicht der DSGVO unterliegen.

1.2 Rollenverteilung (Art 4 DSGVO)

Bei der Verarbeitung von personenbezogenen Daten werden folgende drei Rollen unterschieden: die betroffene Person, die Verantwortlichen und eventuelle Auftragsverarbeiter.

Die betroffene Person ist jene Person, die aufgrund der Daten identifiziert werden kann. Dies betrifft etwa Teilnehmende an Citizen Science-Projekten. Es können aber auch unbeteiligte Dritte sein, wenn Menschen im öffentlichen Raum beobachtet und Daten erhoben werden.

Die Verantwortlichen sammeln und verarbeiten personenbezogene Daten und entscheiden, was mit den Daten passiert. Das heißt, sie treffen die wesentlichen Entscheidungen über Zweck und Mittel der Verarbeitung, sind rechtlich verantwortlich und für den Schutz der Daten zuständig.

Die oder der Verantwortliche ist meist die Citizen Science-Projektleitung. Es können auch mehrere Personen für diese Rolle ausgewählt werden, allerdings muss dann die Verantwortung vertraglich aufgeteilt und festgehalten werden. Datenschutzbeauftragte sind nicht dazu da, die Rolle des Verantwortlichen einzunehmen. Ihre Aufgabe besteht in der Beratung der Verantwortlichen und in der Überwachung der Datenverarbeitung.

Die dritte Rolle der Auftragsverarbeiter haben jene Personen inne, die im Auftrag des oder der Verantwortlichen die gesammelten Daten verarbeiten. Diese Personen sammeln keine Daten, sondern arbeiten nur mit jenen Daten, die bereits gesammelt wurden. Das können z.B. Statistikbüros sein, die Daten aufbereiten und wieder an das Projekt zurückschicken, oder auch Online-Plattformen, die Daten aus einer App verarbeiten.

1.3 Rechte der betroffenen Personen

Einer der Kerninhalte der DSGVO sind die Rechte der betroffenen Personen. Sie dienen dem Schutz jeder Person, deren Daten verarbeitet werden. Hier werden folgende wesentliche Rechte unterschieden (Art 12 ff, Art 16, Art 17, Art 18, Art 20, Art 21 DSGVO):

- Recht auf Auskunft: Betroffene Personen haben das Recht zu erfahren und nachzufragen, welche Daten, die sie selbst betreffen, verarbeitet werden.
- Recht auf Berichtigung falscher Daten: Betroffene Personen haben das Recht, falsche Angaben und Daten richtig stellen zu lassen.
- Recht auf Löschung: Betroffene Personen haben das Recht, die Löschung ihrer personenbezogenen Daten zu verlangen. Diese Daten bzw. der Personenbezug zu den Daten müssen gelöscht werden.
- Recht auf Einschränkung der Verarbeitung: Betroffene Personen haben das Recht, die Verarbeitung ihrer personenbezogener Daten einzuschränken.
- Recht auf Datenübertragbarkeit: Betroffene Personen haben das Recht, ihre personenbezogene Daten anzufordern, um sie anderen zur Verfügung zu stellen.
- Widerspruchsrecht: Dieses Recht steht im Zusammenhang mit dem Recht auf Löschung. Betroffene Personen haben das Recht, der Verarbeitung ihrer personenbezogenen Daten zu widersprechen.

Betroffene Personen müssen spätestens in der Einverständniserklärung auf ihre Rechte hingewiesen werden.

1.4 Besonderheiten beim Recht auf Löschung und Widerrufsrecht

Betroffene Personen haben ein Recht auf die Löschung ihrer personenbezogenen Daten, es sei denn die Löschung der Daten gefährdet die Projektziele. Dies ist auch im Forschungsorganisationsgesetz (FOG) geregelt.

Ob das Recht auf Löschung bzw. Widerruf die Ziele eines wissenschaftlichen Forschungsprojektes behindern würde muss im Einzelfall entschieden werden. Es werden die Interessen der betroffenen Person und das öffentliche Interesse an den Ergebnissen des Forschungsprojektes abgewogen.

Achtung: Wenn eine Einwilligungserklärung widerrufen wird, müssen alle personenbezogenen Daten der betroffenen Person gelöscht werden. Das umfasst auch die Einwilligungserklärung und den Widerruf selbst.

1.5 Grundsatz der Datenminimierung und Speicherbegrenzung

Die Datenschutzgrundverordnung räumt nicht nur den Betroffenen Rechte zur Löschung ein, sondern sieht auch eine beschränkte Zeit für die Speicherung von Daten vor (Art 5). Demnach müssen alle personenbezogenen Daten ab dem Zeitpunkt gelöscht werden, ab dem sie nicht mehr gebraucht werden. Sie dürfen allerdings dann weiter aufbewahrt werden, wenn sie für wissenschaftliche Zwecke zu einem späteren Zeitpunkt wieder benötigt werden. Hier muss die Wissenschaftlichkeit bzw. Notwendigkeit einer weiteren Speicherung nachgewiesen werden können. Das Forschungsorganisationsgesetz hat eine Frist von 10 Jahren für die Speicherung von Daten festgelegt.

Tipp: Daten, die keinen Personenbezug aufweisen, unterliegen nicht der DSGVO. Es ist daher ratsam, Daten so weit wie möglich ohne Personenbezug zu speichern und anonyme Daten für die weitere Verarbeitung zu nutzen.

1.6 Rechtmäßigkeit der Verarbeitung

Der Artikel 6 Absatz 1 der Datenschutzgrundverordnung regelt die Rechtmäßigkeit der Verarbeitung personenbezogener Daten, also wann eine Verarbeitung rechtmäßig erfolgt. Hier gilt, dass jegliche Handlung, die sich auf personenbezogene Daten bezieht, als Verarbeitung gewertet wird. Dies umfasst neben der Speicherung oder Auswertung unter anderem auch die Löschung oder Auflistung.

Die Rechtmäßigkeit der Verarbeitung ist gegeben, wenn einer der folgenden Punkte erfüllt ist:

- Einwilligung der betroffenen Personen
- Vertragserfüllung
- Erfüllung einer rechtlichen Verpflichtung
- Lebenswichtige Interessen
- Aufgabe im öffentlichen Interesse
- Berechtigtes Interesse des Verantwortlichen

Für Citizen Science Projekte wird häufig eine Einwilligungserklärung notwendig sein, vor allem wenn personenbezogene Daten nicht ausschließlich zu wissenschaftlichen Zwecken, sondern z.B. auch zur Mitgliederverwaltung verwendet werden sollen. Wichtig ist zu beachten, dass die Einwilligung explizit erfolgen muss. Eine implizite Einwilligung reicht nicht aus.

Die weiteren, gelisteten Möglichkeiten, die eine Rechtmäßigkeit der Verarbeitung ermöglichen, treffen meist nicht auf Citizen Science-Projekte zu. So haben die meisten Citizen Science-Projekte keine Aufgabe im (ausschließlich) öffentlichen Interesse oder rechtliche Verpflichtungen gegenüber den betroffenen Personen zu erfüllen. Die Vertragserfüllung bezieht sich in der DSGVO meist auf Verträge, bei denen Geschäfte

abgewickelt werden und monetäre Aufwendungen vorliegen. Das berechnigte Interesse der Verantwortlichen kann bei Forschungsprojekten zutreffen, muss aber wie die Aufgabe im öffentlichen Interessen im Einzelfall ermittelt werden.

1.7 Öffnungsklauseln und Forschungsorganisationsgesetz (Art 89 DSGVO)

In der europaweit gültigen Datenschutzgrundverordnung wurde den EU-Mitgliedsstaaten Spielraum zur Selbstbestimmung durch Öffnungsklauseln eingeräumt, die es ihnen ermöglichen, die DSGVO durch eigene Regelungen und Gesetze zu präzisieren. Mit einem Zusatz aus dem Jahr 2018 zum Forschungsorganisationsgesetz (FOG), der unter anderem die Datenverarbeitung zu Forschungszwecken im öffentlichen Interesse regelt, wurden ergänzende Richtlinien zur DSGVO für die Wissenschaft und Forschung in Österreich festgelegt. Es ist zu hoffen, dass das FOG in seiner Fassung von 2018 noch nachgeschärft werden wird. So ist etwa unklar, was genau unter dem Begriff „wissenschaftliche Forschung im öffentlichen Interesse“ fällt.

Das FOG besagt unter anderem, dass für Citizen Science-Projekte eine Einwilligungserklärung unter bestimmten Umständen nicht zwingend erforderlich ist. Aber auch in diesen Fällen müssen Projekte zu Beginn des Projekts über den Umfang, die Dauer, die Verarbeitung und die Art der personenbezogenen Daten informieren und diese auch ausdrücklich und nachweisbar kommunizieren (§2i Abs 4 FOG).

2 Praktische Umsetzung in 8 Schritten

Die DSGVO bringt einige Neuerungen für Forschungsprojekte. Annemarie Hofer präsentierte im Rahmen ihres Vortrages einen 8-Schritte-Plan, der Citizen Science-Projekte im Umgang mit der DSGVO unterstützen soll.

1. Punkt: **Zuständigkeiten klären!**

Wer übernimmt im Projekt die Rolle des Verantwortlichen, also jener Person, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten entscheidet?

Im ersten Schritt sollte zudem auch überlegt werden, ob es Auftragsverarbeitende geben soll. Zusätzlich sollten Aufgaben, Zuständigkeiten und Zugriffsmöglichkeiten festgelegt und dokumentiert werden.

2. Punkt: **Welche Daten fallen an?**

Nachdem die Zuständigkeiten geklärt sind, sollte man sich überlegen, welche Daten für das Projekt gesammelt werden und ob es sich dabei um personenbezogene Daten handelt.

Hier kann eine Tabelle hilfreich sein, die alle Schritte des Forschungsprojektes

darstellt, sowie alle Daten auflistet, die in den einzelnen Schritten gesammelt und verarbeitet werden. Wichtig ist dabei, auch mögliche Verknüpfungen zu bedenken, durch die sich personenbezogene Daten ergeben könnten. Anonyme Daten müssen nicht ins Verarbeitungsverzeichnis, pseudonyme Daten hingegen müssen im Verzeichnis angeführt werden.

Es sollte darauf geachtet werden, alle Personen, die an dem Projekt beteiligt sind, in diesen Schritt zu involvieren. Dieser Vorgang wird bei vielen Projekten mehrfach wiederholt werden müssen, da sich oftmals Änderungen im Projekt ergeben.

3. Punkt: **Welche Verarbeitungsschritte werden vorgenommen?**

Als nächsten Schritt sollte man überlegen, welche Daten von wem wie verarbeitet werden. Auch der Zweck der Verarbeitung der Daten sollte bereits zu Beginn eines Projekts festgelegt und bekannt gegeben werden.

Wichtig zu bedenken wäre, ob Daten während des Projekts eventuell in ein Drittland – außerhalb der EU oder des Safe Harbor-Abkommens – übermittelt werden. Dies kann etwa durch die Verwendung eines (Cloud)-Servers passieren.

Zudem sollte man sich, basierend auf dem Grundsatz der Datenminimierung, nochmals Gedanken über die gesammelten Daten machen: Sind alle Daten wirklich essentiell für das Projekt oder kann das Forschungsziel auch ohne personenbezogene Daten erreicht werden? Wenn diese Daten nicht unbedingt notwendig sind, so sollten sie nicht erhoben werden. Dies ist vor allem für die Aufbewahrung und Sicherheit ein wichtiger Aspekt, denn Daten, die nicht gesammelt oder gespeichert werden, müssen nicht geschützt werden.

4. Punkt: **Sicherheitsmaßnahmen und Aufbewahrungsdauer**

Personenbezogene Daten müssen auf angemessene Art und Weise gesichert werden. Diese Aufgabe obliegt den Verantwortlichen eines Projekts. Hier gilt es festzulegen, wer auf welche Weise welche Daten verwaltet. Wer hat Zugriff auf die Daten? In welchem Land oder über wen wird der Server betrieben, auf dem die Daten gesichert werden? All diese Punkte sind zu bedenken.

Zudem sind der Stand der Technik aber auch Art, Umfang und Zweck der Verarbeitung zu berücksichtigen. Dabei sollten Projekte die Implementierungskosten und eine vertretbare Relation zwischen Kosten und Sensibilität der Daten abwägen. Bei einer Auslagerung der Datenauswertung oder -speicherung muss der Verantwortliche zudem nach bestem sicher sein können, dass die Sicherheit bei der dritten Institution gewährleistet werden kann.

Neben der Datensicherheit muss auch der Grundsatz der Speicherbegrenzung mitbedacht werden, nach der personenbezogene Daten nur so lange gespeichert werden dürfen, so lange sie gebraucht werden. Sobald der Nutzen des Personenbezugs nicht mehr gegeben ist, muss dieser entfernt werden.

5. Punkt: **Datenschutzerklärung formulieren** (Privacy Notice)

Die Datenschutzerklärung muss ab dem Zeitpunkt der Datensammlung zur Verfügung stehen. Darin müssen folgende Punkte angeführt sein:

- Name und Kontakt des Verantwortlichen
- Zweck der Verarbeitung der personenbezogenen Daten und deren Rechtsgrundlage
- Empfänger, wenn Daten übermittelt werden sollen; sofern Daten in ein Drittland übermittelt werden, Informationen zur jeweiligen Rechtsgrundlage
- Aufbewahrungsdauer der jeweiligen Daten
- Rechtsansprüche der betroffenen Personen auf Auskunft, Berichtigung, Löschung bzw. Einschränkung sowie Widerspruch
- Information zum Beschwerderecht bei der Aufsichtsbehörde

Die Artikel-29-Datenschutzgruppe empfiehlt, auf Webseiten in 3 Layern auf die Datenschutzerklärung hinzuweisen bzw. über diese zu informieren.

Layer 1: Hinweis auf die Datenschutzerklärung mit einem Link zur gesamten Erklärung

Layer 2: Kurzfassung der Datenschutzerklärung mit den wichtigsten Punkten

Layer 3: Gesamte Datenschutzerklärung

6. Punkt: **Einwilligungserklärung formulieren**

Die Einwilligungserklärung muss eine freiwillige, aktive und eindeutig bestätigende Handlung sein (Art 4 Z 11), d.h. Projekte müssen im Zweifelsfall nachweisen können, dass die Person aktiv zugestimmt hat. So sind etwa Zustimmungen, die online erfolgen, nicht mehr durch bereits vorab angekreuzte Kästchen möglich.

Eine Einwilligungserklärung muss zudem fallspezifisch erstellt werden (Art 5 Abs 1).

In der Einwilligungserklärung müssen die Identität des Verantwortlichen, der Verarbeitungszweck der Daten und auch ein Hinweis auf das Widerrufsrecht enthalten sein (Art 28 Abs 1).

7. Punkt: **Verzeichnis der Verarbeitungstätigkeiten (Art 30)**

Das Verzeichnis der Verarbeitungstätigkeiten ist ein internes Verzeichnis und muss den betroffenen Personen nicht zur Verfügung gestellt werden. Nur auf Anfrage einer Behörde muss das Verzeichnis vorgelegt werden, in dem aufgezeigt wird, wie die gesammelten Daten verarbeitet werden.

Das Verzeichnis der Verarbeitungstätigkeiten darf auch elektronisch geführt werden und umfasst folgende Punkte:

- Name und Kontaktdaten des Verantwortlichen
- Verarbeitungszwecke und deren Rechtsgrundlage
- Beschreibung der Kategorien betroffener Personen (z.B. Teilnehmende)
- Beschreibung der Kategorien personenbezogener Daten (z.B. Adressdaten, Alter, Ausbildung, Geschlecht)

- Kategorien der Empfänger, wenn gegeben (z.B. projektübergreifende Plattformen)
- Speicherdauer der einzelnen Datenkategorien
- Beschreibung der Datensicherheitsmaßnahmen

8. Punkt: **Einhaltung der Betroffenenrechte sicherstellen**

Zudem sollte die Einwilligung der betroffenen Personen schriftlich vorliegen und nicht auf mündlicher Basis passieren, da die Einwilligung nachgewiesen werden können muss.

Wichtig ist, dass die Datenschutzerklärung, die Einwilligungserklärung wie auch das Verarbeitungsregister selbst formuliert werden und auf das eigene Projekt abgestimmt sein müssen. Ein Kopieren von anderen ist nicht zu empfehlen, weil dadurch wichtige Punkte im eigenen Prozess übersehen werden können.

3 Weitere Anforderungen

Neben der Datenschutzgrundverordnung gibt es noch zusätzliche rechtliche Anforderungen, die von Citizen Science-Projekten beachtet werden sollten. Dazu zählt etwa das Urheberrecht, das die Verwendung von Bildern regelt. Mit der CC0-Lizenz können Bilder zwar freigegeben werden, auf das Urheberrecht kann man in Österreich aber nicht verzichten und dieses kann auch nicht aufgehoben werden. Nähere Informationen dazu gibt es hier: <https://www.creativecommons.at/cc0-lizenz-oesterreich>

Weitere wichtige rechtliche Anforderungen sind das Recht am eigenen Bild, die Rechte Dritter oder die Offenlegungspflicht, wie die Medien- und Telekommunikationsrechte, zu Impressum, Cookie-Richtlinien, etc.

Diese Richtlinien und Gesetze zählen zwar nicht zur Datenschutzgrundverordnung, müssen aber dennoch in Citizen Science-Projekten berücksichtigt werden.