Castellum – eine datenschutzkonforme Webanwendung für das Management von Proband:innen der wissenschaftlichen Forschung

Castellum – a privacy-compliant web application for the management of study participants in scientific research

Karolina Luisa Mader[1]
Philipp Harlos[1]
Tobias Bengfort[1]

1 Max-Planck-Institut für Bildungsforschung, Berlin, Deutschland

Abstract

Strict requirements apply to the administration of participants in regulated clinical trials. Depending on the study, medicines acts, the Medical Device Law Implementation Act as well as the guidelines and standards of good clinical practice must be complied with or implemented. Even outside the clinical research area, there are clear requirements regarding the administration of participants and the processing of their personal data, particularly in the human sciences, at the latest since the European Data Protection Regulation came into force in 2018. In order to meet these requirements, the Castellum software has been developed at the Max Planck Institute for Human Development since 2016 and has been used successfully since May 2020. Castellum is a turnkey open-source web application for the data protection-compliant management of participants and their data.

The use of Castellum has so far been particularly successful for institutions conducting research in the humanities that carry out several studies in parallel, that want to proactively recruit participants from an internal pool of interested persons after they have given their consent (recruitment consent), and that generate data when dealing with these participants.

The rules that apply to the clinical research area have not been a priority in the development of Castellum to date. The reason is that Castellum has not yet been used in the clinical research area and thus there was no need to adapt the system to the rules. However, medical research institutions have expressed interest in Castellum in the recent past. On the one hand, this may be due to the fact that no comparable open-source project exists. On the other hand, Castellum was explicitly designed to be flexible and expandable enough to be adaptable to the workflows and processes of other research institutions. Since Castellum is subject to the AGPL licence, the software may be used free of charge without restrictions.

The main focus during development was on compliance with the General Data Protection Regulation and other aspects of general IT security. For this reason, we believe it is possible that Castellum is also suitable for contexts that work with highly sensitive data, such as medical research institutions. This opens up a new space for discussion: How can Castellum be used in the clinical regulated field? Which conditions of regulated research studies does Castellum currently fulfil and which not yet? What does Castellum need in order to implement the guidelines on good clinical practice? Which adaptations and extensions are necessary for Castellum to comply with the regulations, rules and laws of regulated studies?

We are very interested in introducing Castellum in the clinical research field. From our point of view, it is important to examine within a cooperative process for which purposes Castellum is already qualified in the clinical research area and which adaptations still need to be implement-

ed. We are striving to jointly identify suitable measures to validate Castellum, especially for regulated clinical research studies.
This article first presents what Castellum is currently able to offer. It then focuses on a possible expansion of the software in the clinical research area.

Keywords: Castellum, General Data Protection Regulation, data protection, open source software, subject management, study recruitment, medical research studies

Zusammenfassung

Bei der Verwaltung von Proband:innen in regulierten klinischen Studien gelten strenge Vorgaben. Je nach Studie gilt es die Clinical Trials Regulation, das Medizinprodukterecht-Durchführungsgesetz, ggf. die jeweils gültige Berufsordnung sowie die Leitlinien und Normen der guten klinischen Praxis einzuhalten bzw. umzusetzen. Auch außerhalb des klinischen Forschungsbereichs existieren insbesondere in den Humanwissenschaften spätestens seit Inkrafttreten der Europäischen Datenschutzgrundverordnung im Jahre 2018 klare Vorgaben bzgl. der Verwaltung von Proband:innen und der Verarbeitung ihrer personenbezogenen Daten. Um diesen Vorgaben gerecht zu werden, wurde am Max-Planck-Institut für Bildungsforschung seit 2016 die Software Castellum entwickelt und wird seit Mai 2020 erfolgreich eingesetzt. Hierbei handelt es sich um eine schlüsselfertige Open-Source-Webanwendung für das Management von Proband:innen und ihren Daten.
Der Einsatz von Castellum hat sich bisher insbesondere für humanwissenschaftlich forschende Einrichtungen bewährt, die parallel mehrere Studien durchführen, die proaktiv Proband:innen aus einem internen Pool studieninteressierter Personen nach Einwilligung (Rekrutierungseinwilligung) rekrutieren möchten und bei denen im Umgang mit diesen Proband:innen Daten anfallen.
Die für den klinischen Forschungsbereich geltenden Regeln stellten in der Entwicklung von Castellum bis heute keine Priorität dar. Der Grund liegt darin, dass Castellum bisher nicht im klinischen Forschungsbereich eingesetzt wird und daher keine Notwendigkeit bestand, das System an die Regeln anzupassen. Medizinische Forschungseinrichtungen haben allerdings in der jüngeren Vergangenheit Interesse an Castellum bekundet. Dies mag zum einen daran liegen, dass kein vergleichbares Open-Source-Projekt existiert. Andererseits wurde Castellum explizit so flexibel und ausbaufähig konzipiert, dass es an die Arbeitsabläufe und Prozesse anderer Forschungseinrichtungen anpassbar ist. Da Castellum der AGPL-Lizenz unterliegt, darf die Software ohne Einschränkungen kostenfrei verwendet werden.
Das Hauptaugenmerk lag bei der Entwicklung auf der Einhaltung der Datenschutzgrundverordnung und anderen Aspekten der allgemeinen IT-Sicherheit. Aus diesem Grund halten wir es für möglich, dass Castellum auch für Kontexte geeignet ist, die mit hochsensiblen Daten arbeiten, wie z.B. medizinische Forschungseinrichtungen. Dadurch öffnet sich ein neuer Diskussionsraum: Wie kann Castellum im klinisch regulierten Bereich eingesetzt werden? Welche Bedingungen regulierter Forschungsstudien erfüllt Castellum aktuell und welche noch nicht? Was bedarf Castellum, um die Leitlinien zur guten klinischen Praxis umzusetzen? Welche Anpassungen und Erweiterungen sind nötig, damit Castellum die Verordnungen, Regularien und Gesetze regulierter Studien einhält?
Wir sind sehr daran interessiert, Castellum im klinischen Forschungsbereich einzuführen. Aus unserer Sicht gilt es in einem kooperativen Prozess zu prüfen, für welche Einsätze Castellum im klinischen Forschungsbereich bereits qualifiziert ist und welche Anpassungen noch

umzusetzen sind. Wir sind bestrebt, gemeinsam geeignete Maßnahmen zu identifizieren, um Castellum insbesondere für regulierte klinische Forschungsstudien zu validieren.
Dieser Artikel stellt zunächst dar, was Castellum nach aktuellem Stand leisten kann. Anschließend richtet sich der Fokus auf eine mögliche Ausweitung der Software im klinischen Forschungsbereich.

Schlüsselwörter: Castellum, Datenschutzgrundverordnung, Datenschutz, Open-Source-Software, Proband:innen-Management, Studienrekrutierung, medizinische Forschungsstudien

1 Datenschutzrechtliche Anforderungen an das Proband:innen-Management forschender Einrichtungen

Spätestens seit Inkrafttreten der Europäischen Datenschutzgrundverordnung (DSGVO) und des überarbeiteten Bundesdatenschutzgesetztes im Jahr 2018 gelten für die Verarbeitung personenbezogener Daten strenge Richtlinien. Die Umsetzung der gesetzlichen Vorgaben ist durch angemessene technische und organisatorische Maßnahmen zu gewährleisten. Die Angemessenheit richtet sich dabei unter anderem nach dem entsprechenden Schutzbedarf der Daten sowie der Art und Weise der Datenverarbeitung. Dies stellt insbesondere humanwissenschaftliche Forschungseinrichtungen vor neue Herausforderungen bei der Rekrutierung von Proband:innen und der Verarbeitung der dazugehörigen (personenbezogenen) Daten.
Werden die Regelungen der DSGVO nicht eingehalten, können finanzielle, strukturelle und auch rufschädigende Konsequenzen eintreten. Diese können sich wiederum negativ auf den gesamten wissenschaftlichen Betrieb einer Forschungseinrichtung auswirken. Gleichzeitig besteht bei Forschenden der Wunsch nach einer benutzerfreundlichen, digitalen Anwendung, welche die Verwaltung von Proband:innen-Daten vereinfacht und damit den Forschungsprozess effizient unterstützt. An vielen Einrichtungen fehlen jedoch sowohl die Ressourcen als auch die Expertise, um eine nachhaltige und anwendungsorientierte Lösung umzusetzen. Das Castellum-Projekt hat sich den genannten Herausforderungen gestellt und unterstützt bisher einige humanwissenschaftliche Forschungseinrichtungen bei der Umsetzung datenschutzkonformer Studienprozesse. Mit aktuellem Stand erfüllt die Software allerdings (noch) nicht die Verordnungen, Regularien und Gesetze, denen regulierte klinische Forschungsstudien unterliegen.

2 Vorteile von Castellum

Castellum (https://castellum.mpib.berlin) wurde am Max-Planck-Institut für Bildungsforschung (MPIB) seit 2016 entwickelt. Hierbei handelt es sich um eine schlüsselfertige Open-Source-Webanwendung für die datenschutzkonforme Verwaltung von Proband:innen und ihren Daten, die sich bislang insbesondere in den Humanwissenschaften bewährt hat. Das Tool kann Einrichtungen unterstützen, die parallel mehrere Studien durchführen, die proaktiv Proband:innen aus einem internen Pool studieninteressierter Personen nach deren Einwilligung rekrutieren möchten [1] und bei denen im Umgang mit diesen Proband:innen Daten anfallen.
Castellum ermöglicht es Forschenden, Informationen über Studieninteressierte und Proband:innen optimal zu organisieren. Somit werden u.a. die Studienrekrutierung, die Terminverwaltung und die Studiendurchführung vereinfacht.
Insbesondere bei der Arbeit mit sensiblen personenbezogenen Daten sollten Mittel gefunden werden, um diese Daten vor internem Missbrauch zu schützen. Dies ist mit Hilfe von Castellum umsetzbar, da die Anwendung angemessene technische sowie organisatorische Maßnahmen integriert. So ist der Zugriff auf Castellum über eine Zwei-Faktor-Authentifizierung geschützt. Die einsetzenden Institutionen haben die volle Kontrolle über die Daten, da sie auf der eigenen Serverinfrastruktur vorgehalten werden und nicht auf Cloud-Diensten. Gleichzeitig vereinfacht Castellum die Verwaltung von Proband:innen-Daten durch ein hohes Maß an Nutzerfreundlichkeit und unterstützt somit den gesamten Forschungsprozess effizient.

3 Entwicklungsgeschichte und Einsatz an Forschungsinstituten

Die Entwicklung von Castellum fand in enger Abstimmung mit dem wissenschaftlichen Personal des MPIBs sowie der Datenschutzbeauftragten der Max-Planck-Gesellschaft statt. Gemeinsam wurden Anwendungsfälle in den Humanwissenschaften definiert und daraus konkrete Anforderungen an die Software abgeleitet. Somit finden in Castellum relevante Aspekte der Regeln guter wissenschaftlicher Praxis Berücksichtigung und die Anwendung ist gut in den Forschungsalltag integrierbar. Das Hauptaugenmerk lag auf der Einhaltung der DSGVO und Aspekten der allgemeinen IT-Sicherheit [1].
Castellum ist seit Mai 2020 erfolgreich im produktiven Einsatz am MPIB. Fortlaufend werden von den Anwender:innen unterschiedlicher Bereiche neue Anforderungen an die Software erhoben. Da die Weiterentwicklung auf der agilen SCRUM-Methode beruht, können diese Anforderungen innerhalb dreiwöchiger Sprints schnell umgesetzt werden. Handelt es sich um größere Veränderungen

oder komplett neue Funktionen, werden diese entwickelt und zunächst im Rahmen von Usability-Tests überprüft und ggf. angepasst, bevor sie in die Software integriert werden. Mit diesem Ansatz macht Castellum die Datenverwaltung zukunftssicher und kann sich den verändernden Forschungsanforderungen und technologischen Fortschritten anpassen.

Seit September 2021 wird Castellum am Max-Planck-Institut für biologische Kybernetik eingesetzt sowie seit Beginn des Jahres 2023 am Ernst Strüngmann Institut in Frankfurt im Rahmen zweier Pilotprojekte getestet. Doch auch an anderen Einrichtungen werden Defizite im Bereich des Proband:innen-Managements festgestellt und die Notwendigkeit einer umfassenden Softwarelösung gesehen. Vermutlich vor dem Hintergrund, dass kein vergleichbares Open-Source-Projekt existiert, welches dieses breite Anwendungsspektrum abdeckt, haben bereits weitere Einrichtungen Interesse an Castellum bekundet oder bereits erste Schritte unternommen, um Castellum zur Unterstützung ihres Forschungsprozesses langfristig zu implementieren. Dazu gehören die Fakultät für Wirtschaftswissenschaft der Bergischen Universität Wuppertal, das Department of Psychology and Logopedics der Universität Helsinki, die Carl von Ossietzky Universität Oldenburg, die Fachhochschule Potsdam, das Universitätsklinikum Hamburg-Eppendorf sowie die Fakultät für Psychologie und Bewegungswissenschaft der Universität Hamburg.

4 Management der Daten, Rollen und Rechte

Castellum stellt eine klar definierte Struktur für den Umgang mit den (personenbezogenen) Daten aller Proband:innen bereit. Kontaktinformationen (z.B. Name und postalische Adresse), Rekrutierungsmerkmale (z.B. Alter und Bildungsabschluss) und Prozessinformationen (z.B. vorhandene Einwilligungen und aktuelle Erreichbarkeiten) werden in Castellum gespeichert [1]. Wissenschaftliche Daten und Werte, die nach Studienprotokoll erhoben werden, werden dagegen außerhalb von Castellum abgelegt. Die Speicherung sollte in einem für die spezifischen Studientypen qualifizierten EDC-System erfolgen (vgl. Abschnitt 5.3).

Neue Castellum-Nutzer:innen können über LDAP-Gruppen importiert und ihnen dann verschiedene Rollen innerhalb der Anwendung zugewiesen werden. Aktuell deckt Castellum fünf globale Rollen ab. Namentlich gehören dazu die Datenschutzkoordinator:innen, die Principal Subject Manager:innen, die Rezeptionist:innen, die Studienkoordinator:innen und die Study Approver.

In Castellum eingetragene Datenschutzkoordinator:innen und Principal Subject Manager:innen erhalten einen umfassenden Zugriff auf die Daten (potenzieller) Proband:innen, um die mit den Rollen verknüpften Aufgaben und Verantwortlichkeiten umsetzen zu können. Aus diesem Grund sollten diese Rollen nur einer sehr kleinen Gruppe von Personen zugewiesen werden. Die entsprechenden Informationen sollten transparent in den Rekrutierungseinwilligungen der jeweiligen Einrichtung dargestellt werden.

Ein:e für datenschutzrechtliche Belange in Castellum abgestellte:r Datenschutzkoordinator:in nutzt die von Castellum dargebotene, zentrale Übersicht, um die DSGVO-Betroffenenrechte („Betroffene“ hier im Sinne der Proband:innen) fristgerecht umzusetzen. Dazu gehören beispielsweise Anfragen zur Datenlöschung gemäß Artikel 17 DSGVO und Anfragen zur Datenauskunft gemäß Artikel 15 DSGVO. Macht eine in Castellum als studieninteressiert gelistete Person von einem dieser Rechte Gebrauch, indem sie beispielsweise in der Einrichtung anruft und um Datenlöschung bittet, kann dieses Löschgesuch direkt in Castellum vermerkt werden. Die Person taucht anschließend im Datenschutz-Dashboard mit allen relevanten Informationen auf. Somit sind alle Anfragen übersichtlich an einer zentralen Stelle abgebildet und können schnell von der Datenschutzkoordination umgesetzt werden. Bei Studien, die bestimmten Gesetzen und Regularien unterliegen, dürfen Daten allerdings auch bei Widerruf nicht gelöscht werden. Diese Anforderung ist bisher nicht technisch in Castellum abgebildet. Denkbar wäre eine interne Umsetzung allerdings durch einen organisatorischen Prozess, bei dem klar definierte Vermerke zu den Löschbestimmungen von Daten bei den einzelnen Studientypen hinterlegt werden. Datenschutzkoordinator:innen stellen zudem sicher, dass alle aufgeführten (potenziellen) Proband:innen eine zulängliche Rechtsgrundlage aufweisen.

Ein typischer Anwendungsfall im Bereich des Subject Managements sieht folgendermaßen aus: Die Erstkontaktperson (in Castellum „Principal Subject Manager“) nimmt die Daten eines Probanden auf, holt seine Einwilligung ein (beispielsweise eine Studieneinwilligung, die das Interesse zur Teilnahme an einer spezifischen Studie bekundet oder eine Rekrutierungseinwilligung, um den Probanden zu Studienzwecken zu kontaktieren) und hinterlegt einen Basisdatensatz in Castellum [2]. Mögliche Duplikate können bereits an dieser Stelle durch einen Datenabgleich vermieden werden.

Rezeptionist:innen erhalten eine Übersicht über alle anstehenden Testungstermine des jeweiligen Tages, um in der Einrichtung ankommende Proband:innen an den richtigen Testungsort schicken zu können.

Studienkoordinator:innen sind für das Anlegen der Studien in Castellum zuständig. Dabei werden wichtige Angaben für die Rekrutierung gemacht (z.B. Festlegung des Rekrutierungstextes und des Testungszeitraums) sowie für die Studie relevante Ein- und Ausschlusskriterien festgelegt. Diese für die Rekrutierung genutzten Kriterien können von den anwendenden Instituten individuell im Administrationsbereich in Castellum angelegt werden (vgl. Abschnitt 5.1).

Zu Beginn einer Studie kann die Studienkoordination prüfen, ob sich genügend potenzielle Proband:innen in Castellum befinden, abhängig von der prognostizierten Rücklaufquote und den Rekrutierungsfiltern. Personen, welche für die Prüfung der Studie zuständig sind, nehmen

Abbildung 1: In Castellum integriertes Rollen- und Rechtesystem

die Studieneinstellungen in Augenschein. Sind die benötigten Voraussetzungen erfüllt, kann die Studie gestartet werden. Damit wird der Rekrutierungsprozess eingeleitet. Studienkoordinator:innen beenden zudem die Studien nach der Datenerhebung und sind zuständig für das Löschen der Kodierlisten unter Berücksichtigung der geltenden Archivierungsfristen.

Nutzer:innen von Castellum können zwei weitere Rollen (Recruiter und Study Conductor) lokal innerhalb spezifischer Studien zugewiesen werden. Wird eine mitarbeitende Person als Recruiter freigeschaltet, erhält sie ausschließlich Zugriff auf die Kontaktdaten der potenziellen Proband:innen, die den festgelegten Filterkriterien der Studie entsprechen. Dadurch können diese beispielsweise per Telefon oder Mail zu Studienzwecken kontaktiert werden. Mitarbeitende, welche die Testungen durchführen und dabei wissenschaftliche Daten erheben, erhalten Zugriff auf die Kontaktdaten und Pseudonyme der Proband:innen der entsprechenden Studie [1]. Die Nutzung der von Castellum vorgesehenen Rollen- und Rechtestruktur ermöglicht es, dass jede:r Castellum-Nutzer:in lediglich Einsicht in die Daten erhält, die für die Ausführung der entsprechenden Arbeit unabdingbar sind.

Abbildung 1 zeigt die einzelnen in Castellum integrierten Rollen auf und beschreibt in zusammengefasster Form deren Verantwortlichkeiten bzw. Rechte.

5 Integrierte Funktionen

Im Folgenden werden einige Funktionsbeispiele von Castellum aufgelistet und erläutert.

5.1 Rekrutierung von Proband:innen

Neben den Kontaktdaten von Proband:innen können weitere Informationen in Castellum eingepflegt werden, die als Rekrutierungsmerkmale fungieren. Diese können durch die entsprechenden Einrichtungen flexibel ausgewählt werden. Sie sind allerdings individuell zu validieren und verifizieren, damit sie für Rekrutierungsentscheidungen in Studien, die bestimmten Leitlinien unterliegen, tatsächlich genutzt werden können.

Denkbare Rekrutierungsmerkmale umfassen die Händigkeit, Muttersprache sowie den höchsten Bildungsabschluss. Dadurch, dass diese Informationen als Rekrutierungsfilter genutzt werden, wird die Suche nach geeigneten Proband:innen vereinfacht und zeitlich verkürzt. Das Ergebnis ist dann eine Rekrutierungsliste, die potenzielle Proband:innen enthält, welche den definierten Ein- und Ausschlusskriterien entsprechen. Diese Liste ist bereits randomisiert, indem aus allen zutreffenden Datensätzen zufällig Personen ausgewählt und den Recruitern vorgeschlagen werden. Voraussetzung für die Auswahl ist lediglich, dass die potenziellen Proband:innen den Filterkriterien entsprechen und eine gültige Einwilligung zur Kontaktierung besteht.

Den Recruitern stehen ein Rekrutierungstext, der vorab von der Studienkoordination eingepflegt wurde, sowie weitere wichtige Informationen zur Studie für den Rekrutierungsprozess zur Verfügung. Dazu gehören beispielsweise die Dauer und Art der jeweiligen Testsitzungen und besondere Ein- und Ausschlusskriterien. Diese Informationen können an die potenziellen Proband:innen kommuniziert werden um zu prüfen, ob die Personen für die entsprechende Studie geeignet sind. Nach Kontaktierung wird den Personen ein passender Teilnahmestatus zugeordnet, wie z.B. „nimmt teil", „nicht erreicht" oder „ausgeschlossen".
Am MPIB hat es sich bewährt, grob gefasste Filterkriterien wie das Alter, das Geschlecht und die Muttersprache in den Proband:innen-Datensätzen zu halten und für den Rekrutierungsprozess zu nutzen. Im Rekrutierungsgespräch mit den Proband:innen werden dann detailliertere Punkte zur Studientauglichkeit abgefragt. Beispielsweise nutzen Recruiter den MRT-Fragebogen bei der Rekrutierung, sobald es sich um eine MRT-Studie handelt. So wird sichergestellt, dass die Proband:innen tatsächlich MRT-tauglich sind.
Um die Rekrutierungsfunktion von Castellum vollumfänglich nutzen zu können, müssen ggf. interne Prozesse etabliert werden. Beispielsweise können Absprachen mit Statistiker:innen der Studie notwendig sein, um die Population im Rahmen der Stichprobe korrekt abzubilden. Grundsätzlich gilt zunächst zu prüfen, inwiefern durch Castellum die Normen der guten klinischen Praxis eingehalten werden, die für die Rekrutierung von Proband:innen klinischer Studien relevant sind. Wird Castellum für nicht konform mit diesen Normen befunden, können Rekrutierungsentscheidungen ggf. nicht auf Grundlage der Daten aus dem System getroffen werden.

5.2 Erfassung der Rechtsgrundlagen

Aufgrund der Aufgabenstellung von Forschenden, welche unter anderem die Verarbeitung personenbezogener Daten beinhaltet, sind sie verpflichtet, diese Daten nur auf ausdrückliche Weisung der Proband:innen zu verarbeiten. Unbefugt dürfen personenbezogene Daten nicht erhoben, verarbeitet oder genutzt werden. Um dies zu ermöglichen, bietet Castellum einen Überblick über die Rechtsgrundlagen für die Speicherung der Daten eines/einer Proband:in. Hat ein:e Proband:in beispielsweise eine aktuell gültige Version der Rekrutierungseinwilligung unterzeichnet, kann dies im Datensatz der entsprechenden Person in Castellum hinterlegt werden. In diesem Fall darf die Person zu Studienzwecken kontaktiert werden mit dem Ziel, sie zu Studienteilnahmen einzuladen. Unterzeichnete Studieneinwilligungen erlauben die Kontaktierung von Proband:innen im Rahmen der speziellen Studie(-n), für welche die Studieneinwilligung unterschrieben wurde. Zudem ermöglichen Studieneinwilligungen bei longitudinalen Studien, dass nicht für jedes Teilprojekt die Einwilligungen der Proband:innen einzeln erfasst werden müssen. Stattdessen kann die Studienkoordination eine Studie mit mehreren Sitzungen anlegen, für die insgesamt pro Proband:in eine Studieneinwilligung unterschrieben wird. Voraussetzung ist hierbei, dass die Ethikkommission einer übergreifenden Studieneinwilligung sowie der Einwilligung für die Teilprojekte zugestimmt hat.
Im Falle einer ungültigen Rechtsgrundlage einer in Castellum gelisteten Person wird sie im Datenschutz-Dashboard aufgeführt. Der/die Datenschutzkoordinator:in kann daraufhin die Daten der Person löschen bzw. so bearbeiten, dass eine weitere Aufbewahrung datenschutzrechtlich unbedenklich ist. Dies kann z.B. eintreten, wenn eine Studie beendet wurde und somit die Studieneinwilligung an Gültigkeit verliert oder wenn eine Person ihre Rekrutierungseinwilligung zurückzieht.

5.3 Pseudonymisierung und Zugriffsbeschränkungen

Um datenschutzgerechte Lösungen insbesondere im medizinischen Forschungsbereich effizient umzusetzen, sind elementare Prinzipien einzuhalten. Dazu gehört beispielsweise die informationelle Gewaltenteilung. Diese sieht eine getrennte Aufbewahrung und Verwaltung der gespeicherten identifizierenden Personendaten auf der einen und medizinischen Daten auf der anderen Seite vor [2]. Bei typischen Anwendungsfällen ist jedoch eine Verknüpfung personenbezogener Kontaktdaten und elektronischen Proband:innen-Akten, Managementsystemen, Biobanken oder Genomdatenbanken notwendig. Die genannten Anforderungen werden in Castellum durch die Bereitstellung von spezifischen Studienpseudonymen und spezielle Zugriffsbeschränkungen umgesetzt.
Castellum generiert langfristig zuverlässige Pseudonyme für Proband:innen, die individuell innerhalb einer Studie vergeben werden. Dadurch können erhobene wissenschaftliche Daten unter Angabe des Pseudonyms sicher in anderen Systemen abgelegt werden. Diese außerhalb von Castellum abgelegten, wissenschaftlichen Daten können dann lediglich über die Pseudonyme mit den Kontaktdaten der entsprechenden Proband:innen in Castellum verknüpft werden [1]. Die Möglichkeit der Reidentifizierung ist dabei an spezielle Rechte geknüpft. Durch diese Zugriffsbeschränkung wird das Prinzip der Kombination technischer und organisatorischer Sicherheitsmaßnahmen umgesetzt [2].
Mithilfe der Pseudonyme wird die Nutzung externer Anwendungen wie Kalender und (medizinische) Datenbestände ermöglicht, ohne dass sich Klarnamen von Proband:innen außerhalb von Castellum befinden. Auf diese Weise wird ein vertraulicher Umgang mit Informationen umgesetzt, was wiederum das Vertrauen (potenzieller) Proband:innen in wissenschaftliche Einrichtungen und ihre Forschung erhöht [3].
Denkbar ist weiterhin, dass nach der Datenerhebung im Analyseprozess ein Zufallsbefund einer eventuellen Erkrankung festgestellt wird. Da die Datenanalyse außerhalb von Castellum durchgeführt wird, wird an dieser Stelle nur mit den Pseudonymen der Proband:innen gearbeitet. In Castellum kann nun das Pseudonym sicher

aufgelöst werden. Die dadurch offenbar gewordenen Kontaktdaten der Proband:innen können genutzt werden, um ggf. Auskunft über den entsprechenden Befund zu erteilen. Bisher ist in Castellum keine Funktion integriert, die erfasst, in welchen Fällen sich Proband:innen eine Rückmeldung zu Zufallsbefunden wünschen. Ist solch eine Funktion im klinischen Forschungskontext notwendig, könnte sie unter Berücksichtigung der jeweiligen regulatorischen Anforderungen implementiert werden.
Zusätzlich zum integrierten Rollen- und Rechtemanagement werden Zugriffsmöglichkeiten auf Datensätze durch verschiedene Vertraulichkeitsstufen koordiniert. Castellum-Nutzer:innen, Proband:innen sowie einzelnen Attributen werden unterschiedliche Vertraulichkeitsstufen zugewiesen. Dadurch wird sichergestellt, dass Nutzer:innen z.B. nur Datensätze einsehen können, die ihrer individuellen Vertraulichkeitsstufe entsprechen [1].

5.4 Zwei-Faktor-Authentifizierung

In Castellum ist eine eigenständige Zwei-Faktor-Authentifizierung integriert, um die Datensicherheit zu erhöhen. Dabei müssen Castellum-Nutzer:innen einen zusätzlichen Code eingeben, bevor sie sich bei Castellum anmelden können.

6 Technische Details und Informationen zur Installation

Castellum basiert auf dem Open-Source-Webframework Django. Es handelt sich demnach um keine Applikation im klassischen Sinne, die auf jedem Rechner installiert werden muss. Stattdessen stellt Castellum eine webbasierte Anwendung dar, die über den Browser angesteuert wird. Die Software besitzt vergleichsweise niedrige Hardwareansprüche. Um sie aufzusetzen wird lediglich ein Linux System mit mindestens 1 GB Arbeitsspeicher und 2 CPUs benötigt.
Mittlerweile sind alle wichtigen Funktionen verfügbar, sodass sich die Entwicklung auf die Instandhaltung bestehender Funktionen sowie die Integration neuer Funktionsanfragen konzentriert. Dazu werden die Stakeholder aller Institutionen einbezogen, die Castellum einsetzen. Sie werden regelmäßig befragt, inwiefern sich Wünsche zu neuen Funktionen herauskristallisiert haben. Geäußerte Anfragen werden dann gemeinsam besprochen und ggf. in die Weiterentwicklung einbezogen. Durch diesen partizipativen Ansatz wird sichergestellt, dass die technischen Weiterentwicklungen für alle Beteiligten sinnvoll sind. Die Neuerungen werden alle drei Wochen in neuen Versionen von Castellum veröffentlicht. Alle Änderungen am Quellcode lassen sich im Git Repository nachvollziehen. Dort können auch neue Funktionen angefragt oder Probleme gemeldet werden, welche dann ggf. für kommende Updates eingeplant werden. Da Castellum ein Open-Source-Projekt ist, können erfahrene Nutzer:innen auch zum Code beitragen bzw. eine eigene Variante von Castellum entwickeln. Näheres dazu findet sich in unseren Leitlinien: https://git.mpib-berlin.mpg.de/castellum/castellum.
Um einen unverbindlichen ersten Eindruck von Castellum zu erhalten, kann der öffentlich zugängliche Testserver genutzt werden. Dieser ist unter https://castellum.t.mpib-berlin.mpg.de/login/ zu erreichen. Vor der Nutzung empfehlen wir, einen Blick in die Dokumentation zu werfen: https://castellum.mpib.berlin/documentation/en/.
Anders als die reguläre Verwendung von Castellum erfordert die erstmalige Installation technische Kenntnisse, idealerweise Vorwissen im Umgang mit Django. Grundsätzlich empfehlen wir, Castellum als Docker Image zu installieren. Eine detaillierte Anleitung findet sich unter https://git.mpib-berlin.mpg.de/castellum/castellum/-/tree/main/docs/deployment.
Möchte eine Forschungseinrichtung Castellum einsetzen, sollte die Anwendung lokal in dieser gehostet werden. Mithilfe dieses Ansatzes existiert ein zentraler Speicherort, der die Rollen und Rechte der einzelnen Nutzer:innen verwaltet und somit sicherstellt, dass sie lediglich auf Bereiche und Daten Zugriff haben, die sie tatsächlich zur Ausführung ihrer Arbeit benötigen.
Empfehlenswert ist es, Castellum lediglich im Intranet zur Verfügung zu stellen. Das bedeutet, dass ein direkter Zugriff über das Internet nicht möglich sein sollte, um Sicherheitsrisiken zu minimieren. Zudem sollte der Zugang zum Webinterface SSL-verschlüsselt sein (SSL = Secure Sockets Layer). Der Zugriff auf den Server sollte auf eine kleine Gruppe von Administrator:innen der jeweiligen Forschungseinrichtung beschränkt werden [1].
Regelmäßige Sicherungen der Daten von Castellum haben Auswirkungen auf die praktische Umsetzung des Datenschutzes. Denkbar ist ein Szenario, bei dem eine Probandin um die Löschung ihrer Daten bittet. Ihre persönlichen Daten sind auch nach der Löschung noch in einer Sicherung gespeichert. Aus diesem Grund hat es sich für die Humanwissenschaften bisher bewährt, Backups nur für einen klar definierten Zeitraum aufzubewahren, um die Nachvollziehbarkeit der Daten zu gewährleisten. Proband:innen sollten darüber informiert werden, zu welchem Zeitpunkt alle Daten, inklusive des Backups, gelöscht werden [1].

7 Einsatz an weiteren wissenschaftlichen Einrichtungen

Castellum ist AGPL-lizenziert (https://git.mpib-berlin.mpg.de/castellum/castellum/-/blob/main/LICENSE). Somit darf die Software ohne Einschränkungen kostenfrei verwendet werden. Soll eine veränderte Version der Software betrieben werden, ist der Quellcode der Änderungen zu veröffentlichen, damit auch andere davon profitieren können.
Mit Castellum wurde ein Werkzeug geschaffen, das eine datenschutzkonforme Struktur für die Durchführung wissenschaftlicher Studien bietet. Bisher beschränkt sich die Anwendung von Castellum jedoch auf die Humanwissenschaften, wo sich die Anwendung bereits bewährt hat.

Castellum als Open-Source-Projekt wurde von Beginn an flexibel und erweiterbar konzipiert, sodass es mit relativ geringem Aufwand an Arbeitsabläufe und Prozesse anderer humanwissenschaftlicher Forschungseinrichtungen anpassbar ist [1]. Die Software weist ein so breites Anwendungsspektrum auf, dass einzelne Einrichtungen die jeweils ideale Lösung für sich umsetzen können. Unter Berücksichtigung vorhandener IT-Infrastrukturen und Ressourcen kann Castellum kompatibel in gewohnte Arbeitsprozesse eingebunden werden.
Die einzelnen Zugriffsmöglichkeiten und Funktionen sind in Castellum bereits zu sinnvollen Rollen zusammengefasst, die sich in der Humanforschung bewährt haben. Sie sind im gewissen Rahmen jedoch flexibel anpassbar, sodass passgenaue Rollen entwickelt werden können.

7.1 Mögliche Ausweitung im medizinischen Forschungssektor

Aktuell wird das Potenzial festgestellt, Castellum im medizinischen Forschungsbereich auszuweiten. Als flexibel erweiterbares Tool kann die Anwendung Wissenschaftler:innen in Forschungseinrichtungen bei der Verwaltung ihrer Proband:innen unterstützen und stellt dabei den datenschutzkonformen Umgang mit den (personenbezogenen) Daten sicher. So können nichtdatenschutzgerechte Prozesse wie die Proband:innen-Verwaltung mithilfe Datei-basierter Anwendungen wie z.B. MS Excel und MS Access langfristig verhindert werden.
Soll Castellum umfassend mit all seinen Modulen in einer medizinischen Forschungseinrichtung eingesetzt werden, ist klar zu betonen, dass die Anwendung nach aktuellem Stand nicht die benötigten regulatorischen Voraussetzungen erfüllt, denen bestimmte Studientypen im klinischen Forschungskontext unterliegen. Diese sind allerdings oft unabdingbar für die Sicherstellung des Schutzes der Proband:innen und die Datenintegrität. Für einen möglichen Einsatz von Castellum im regulierten Studienbereich müssen wesentliche Anpassungen in der Anwendung vorgenommen und (organisatorische) Maßnahmen getroffen werden, um die Software für den Einsatz im benannten Bereich zu qualifizieren. Diese Anpassungen sollten beispielsweise darauf abzielen, vorgeschriebene Archivierungsfristen einzuhalten. Zudem sollte ein vollständiges Audit-Trail technisch implementiert werden, um die Datenintegrität bei der Durchführung regulierter Studien in ausreichendem Maß sicherzustellen.
Denkbar ist, dass nicht alle von Castellum bereitgestellten Module und Funktionalitäten vollumfänglich von einzelnen Forschungseinrichtungen genutzt werden. Stattdessen könnte Castellum lediglich als Unterstützungstool bei bestimmten Prozessen dienen, z.B. für die reine Proband:innen-Verwaltung.

7.2 Vom Castellum-Team des MPIB geleistete Hilfestellungen

Medizinische Forschungsstudien, insbesondere im regulierten Umfeld, weisen komplexe Anforderungen auf. Durch Castellums Open-Source-Charakter kann die Software an diese spezifischen Anforderungen und Regularien angepasst werden. Das Castellum-Team ist sehr an einem offenen Austausch mit Forschungseinrichtungen des medizinischen Bereichs gelegen, die sich für den Einsatz von Castellum interessieren. Gern stehen wir beratend zur Seite, wenn es darum geht, aus den Studienabläufen in Kliniken und Krankenhäusern neue Anforderungen an Castellum zu erheben. Die Anwendung kann mit aktuellem Stand als Kerngerüst genutzt werden. Dabei sollte Castellum von interessierten Forschungseinrichtungen allerdings derart erweitert werden, dass es ihnen als validiertes System dient und an die lokalen Gegebenheiten (z.B. Vorgaben bestimmter regulierter Studientypen) angepasst ist.
Der Einsatz einer umfassenden neuen Software ist immer auch mit Personal- und Organisationsentwicklungsprozessen verbunden. So müssen beispielsweise Fachkompetenzen aufgebaut und interne Prozesse umgestellt werden. An dieser Stelle unterstützt das Castellum-Team des MPIBs unentgeltlich mit individuellen Beratungsangeboten und bei der Durchführung von Pilotprojekten. Zudem steht unser Team bei Fragen und Anregungen zur (Daten-)Sicherheit, Kompatibilität und zum technischen Einsatz von Castellum selbstverständlich beratend zur Seite.

7.3 Best-Practice-Ansätze

Einrichtungen, die sich für den Einsatz von Castellum entscheiden, sollten organisatorische Prozesse etablieren und Standard Operating Procedures definieren, um eine effiziente Anwendung von Castellum zu gewährleisten. Insbesondere gilt es zu klären, unter welchen Voraussetzungen einzelne Rechte in Castellum vergeben werden, auf welche Weise die Einwilligungen der Proband:innen erhoben und kontrolliert werden und wie die Datenqualität langfristig sichergestellt wird. Die Einrichtungen können dabei von den Erfahrungswerten des MPIBs in Form von bewährten Prozessen und Herangehensweisen profitieren.
Beispielsweise wurden am MPIB erfolgreich organisatorische Prozeduren implementiert, die den Zugriffserlaubnissen neuer Castellum-Nutzer:innen und der Zuweisung bestimmter Rollen vorangehen. So ist ein übergreifendes Datenschutztraining zu absolvieren und ein polizeiliches Führungszeugnis vorzulegen, bevor Testungen mit Kindern durchgeführt werden können.
Bei wichtigen Entscheidungen wird von einem Vier-Augen-Prinzip Gebrauch gemacht. Dies ist beispielsweise der Fall, wenn zu entscheiden ist, ob ein bestimmter Proband oder eine bestimmte Probandin aufgrund von unangemes-

senem Verhalten dauerhaft von Studienteilnahmen ausgeschlossen werden soll.
In der Praxis wurde ein Mehrwert dadurch geschaffen, dass Castellum-Nutzer:innen konstant für datenschutzrechtliche Themen und die korrekte Anwendung von Castellum sensibilisiert werden. Um dies zu erreichen, werden Schulungen durchgeführt, welche theoretische Datenschutzaspekte und die praktische Anwendung vereinen. Bewährte Arbeitsprozesse werden zudem über Mailverteiler sowie speziell für Castellum-Nutzer:innen etablierte Chatkanäle kommuniziert. So wird sichergestellt, dass sich alle Mitarbeitenden über die ordnungsgemäße Ausführung von Routineprozessen im Klaren sind.

8 Fazit und Zukunftsausblick

Castellum bietet viele Vorteile für typische Anwendungsfälle in der humanwissenschaftlichen Forschung. Erstens bietet es eine umfassende Lösung, die vielerlei Funktionen abdeckt und in einer einzigen Anwendung vereint. Dies macht den Einsatz mehrerer Tools und ein Übermaß manueller Prozesse überflüssig. Zweitens ermöglicht der Proband:innen-zentrierte Ansatz eine effiziente Verfolgung und Verwaltung von Informationen über die Proband:innen über mehrere Studien hinweg. Drittens gewährleistet der Pseudonymisierungsdienst die Einhaltung datenschutzrechtlicher Bestimmungen. Zudem wird durch die studienspezifischen Filter die Rekrutierung von Proband:innen vereinfacht, was Ressourcen spart. Letztendlich vereinfacht die Terminverwaltung von Castellum die Planung und Koordination der Testungstermine.
Unser mittelfristiges Ziel ist es, eine aktive Gemeinschaft von Nutzer:innen und Entwickler:innen von Castellum aufzubauen. So sollen ein intensiver Erfahrungsaustausch und die Zusammenarbeit gefördert werden, sodass gemeinsam von Best-Practice-Ansätzen und neuen Ideen profitiert werden kann. Durch eine großflächige Nutzung können datenschutzrechtliche Änderungen zentral umgesetzt werden. Dies würde langfristig zu einer deutlich verbesserten Auslastung von Ressourcen führen.
Zwei zeitnah anstehende Projektmeilensteine stellen die Erstellung eines Organisationshandbuchs sowie eines generischen Train-the-Trainer-Konzepts dar. Die Informationen sollen für Einrichtungen, die Castellum erstmalig einsetzen, zugänglich gemacht werden, um das Wissen über Castellum, seine Implementierung und die korrekte Anwendung nachhaltig zu verankern.
Ein weiteres Ziel ist es, Castellum im klinischen Forschungsbereich zu verbreiten. Dazu gilt es zunächst zu prüfen, inwiefern Castellum bereits für einen Einsatz im benannten Bereich qualifiziert ist und wenn nicht, welche Maßnahmen dafür zu treffen sind. Dazu möchten wir in einen kooperativen Austausch mit klinischen Forschungseinrichtungen treten.

Anmerkung

Interessenkonflikte

Alle an diesem Artikel beteiligten Personen sind Mitarbeitende des Max-Planck-Instituts für Bildungsforschung. Darüber hinaus bestehen keine Interessenkonflikte in Zusammenhang mit diesem Artikel.

Literatur

1. Bengfort T, Hayat T, Göttel T. Castellum: A participant management tool for scientific studies. The Journal of Open Science Software. 2022 Jun;7(79). DOI: 10.21105/joss.04600
2. Pommerening K, Drepper J, Helbing K, Ganslandt T. Leitfaden zum Datenschutz in medizinischen Forschungsprojekten – Generische Lösungen der TMF 2.0. Berlin: Medizinisch Wissenschaftliche Verlagsgesellschaft; 2014.
3. Schaar K. Was hat die Wissenschaft beim Datenschutz künftig zu beachten? Allgemeine und spezifische Änderungen beim Datenschutz im Wissenschaftsbereich durch die neue Europäische Datenschutzgrundverordnung. Berlin: Rat für Sozial- und Wirtschaftsdaten; 2016. (RatSWD Working Paper; 257). DOI: 10.17620/02671.19

Korrespondenzadresse:
Karolina Luisa Mader
Max-Planck-Institut für Bildungsforschung, Lentzeallee 94, 14195 Berlin, Deutschland
mader@mpib-berlin.mpg.de

Bitte zitieren als
Mader KL, Harlos P, Bengfort T. Castellum – eine datenschutzkonforme Webanwendung für das Management von Proband:innen der wissenschaftlichen Forschung. GMS Med Bibl Inf. 2023;23(2):Doc17. DOI: 10.3205/mbi000567, URN: urn:nbn:de:0183-mbi0005676

Artikel online frei zugänglich unter
https://doi.org/10.3205/mbi000567

Veröffentlicht: *19.12.2023*