Universität Basel

Universitätsbibliothek

UNIVERSITÄT BERN

Diese Use Cases sind als eine Hilfestellung für Forschende gedacht. Die Angaben im Text sind rechtlich nicht verbindlich. Bei Fragen zu Datenschutz, Urheberrecht und weiteren Rechtsaspekten wenden Sie sich bitte unbedingt an die zuständigen Stellen Ihrer Universität.

Die Use Cases sind in Zusammenarbeit der Open-Science-Teams der Universitätsbibliotheken Basel und Bern und der Datenschutzbeauftragten der Universität Basel nach der Durchführung eines Workshops zum Thema Datenschutz und Anonymisierung bei qualitativen Forschungsdaten entstanden. Beteiligte Personen:
Silke Bellanger, Christina Besmer, Danielle Kaufmann, Iris Lindenmann, Jennifer Morger, Gero Schreier.

Zitieren als: Bellanger, S. [et al.]: Anonymisieren von Forschungsdaten.
Use Case: Informationssicherheit, 30.10.2020, URL: https://researchdata.unibas.ch/fileadmin/user_upload/researchdata/Documents/UC_Informationssicherheit_20201030.pdf

Informationssicherheit

Use Case

Eine internationale Forschungsgruppe untersucht die Arbeitsbedingungen und -abläufe in asiatischen Textilfabriken. Die Gruppe forscht vor Ort und interviewt Angestellte und Vorgesetzte verschiedener Betriebe. Im Projekt arbeiten nicht nur Universitätsangestellte, sondern auch Hilfskräfte, die ihren privaten Laptop mit ins Feld nehmen. Unterwegs haben sie nur selten Zugang zu einer gesicherten Internetverbindung. Sie rechnen aufgrund früherer Forschungsaufenthalte damit, dass bei der Ausreise aus bestimmten Ländern die Inhalte ihrer Computer bei der Sicherheitskontrolle geprüft oder gelöscht werden. Nach dem Aufenthalt im Feld tauschen sie innerhalb der internationalen Forschungsgruppe ihre Daten aus.

Wie können die Forschenden durch geeignete IT-Massnahmen dafür sorgen, dass Informationen nicht unerlaubt offengelegt werden, keine Forschungsdaten verloren gehen und die Integrität der Daten gesichert ist?

Was ist vor dem Auslandsaufenthalt zu klären?

Wenn mit sensiblen Daten gearbeitet wird, wird dringend empfohlen, bereits bei der Planung des Forschungsprojekts Kontakt mit den zuständigen IT-Abteilungen der Universität und den Informationssicherheitsbeauftragten aufzunehmen und sich beraten zu lassen. Die Projektleitung trägt die Verantwortung für die IT-Sicherheit und muss u. a. gewährleisten, dass auch Projektbeteiligte, die mit privaten Laptops arbeiten, die Sicherheitsauflagen erfüllen. Die IT-Abteilungen können mit Anleitungen und Hinweisen zur Verschlüsselung von Daten und Rechnern behilflich sein. Bei Forschungsaufenthalten im Ausland und internationalen Kooperationen beraten die IT-Abteilungen ebenfalls zu spezifischen Herausforderungen in Zusammenhang mit Datensicherheit. Dabei ist auch abzuwägen, ob die Regierungen der Länder, in denen der Forschungsaufenthalt stattfindet, politisches Interesse an der Untersuchung haben könnten und ob beispielsweise bei der Einreise Beamte versuchen könnten, Spyware auf den Geräten der Forschenden zu installieren. Für den Fall, dass die Forschenden im Ausland IT-Unterstützung benötigen, sollten sie dies vorab mit den IT-Abteilungen abgesprochen und die Kontaktdaten der IT-Abteilung griffbereit haben.

Was sind geeignete Speicherorte für Forschungsdaten bei Forschungsaufenthalten im Ausland?

Lokale Laufwerke auf persönlichen Rechnern, externe Harddisks und USB-Sticks sind nicht geeignet als sichere Speicherorte für Forschungsdaten. Unverschlüsselt sind die Daten auf diesen Medien für Dritte, so sie Zugang zu den Medien haben, bearbeitbar. Das heisst, sie können gelesen, verändert, und gelöscht werden. Die Daten sollten möglichst rasch nach der Erhebung auf einem sicheren Server der Universität oder einer dafür geeigneten Cloud abgelegt werden. Für die Zusammenarbeit in internationalen For-

schungsprojekten können die IT-Abteilungen der Universitäten Tipps zu sicheren Cloud-Anbietern geben. Bevor ein Cloud-Dienst genutzt wird, muss überprüft werden, wo und wie die Daten gespeichert werden und ob der Dienst den Sicherheitsstandards genügt. Für die Zusammenarbeit mit Angehörigen verschiedener Schweizer Universitäten empfiehlt sich zum Beispiel die Verwendung von SWITCHdrive. Sensible Daten müssen für den Transfer und zur Speicherung stets verschlüsselt werden. Nach dem Transfer der Daten auf einen sicheren Server sollten sie auf der lokalen Hardware gelöscht werden. Dabei muss darauf geachtet werden, dass die Daten sicher gelöscht werden; das heisst, dass die Daten nicht ohne weiteres wiederhergestellt werden können. Auch hierzu kann die IT beraten.

Wie können Forschende ihre Forschungsdaten unter Einhaltung des Datenschutzgesetzes transferieren und mit ihren Projektkolleg*innen teilen?

Zu Projektbeginn sollte geklärt werden, welche Forschungsdaten im Projektteam zirkuliert werden. Die Forschungsdaten müssen so früh wie möglich anonymisiert beziehungsweise pseudonymisiert werden und nur die anonymisierten beziehungsweise pseudonymisierten Daten sollten im Projektteam geteilt werden. Die originalen Forschungsdaten sollten möglichst nicht zirkulieren und verschlüsselt oder auf einem anders geschützten Server abgelegt werden. Sofern die Daten pseudonymisiert werden, muss ein sicheres Schlüsselmanagement vorliegen, sodass der Schlüssel zu einer Re-Identifizierung der pseudonymisierten Daten getrennt von den übrigen Daten und mit strikter Zugangsberechtigung aufbewahrt wird. Bei der Datenbearbeitung in internationalen Projektteams sind die Datenschutzgesetze der beteiligten Länder zu beachten. Insbesondere muss bei einem Datentransfer aus der Schweiz ins Ausland gewährleistet sein, dass diese Daten im jeweiligen Land durch entsprechende Datenschutzgesetze angemessen geschützt sind. Wenn ein Land über einen ungenügenden Datenschutz verfügt, müssen die Projektpartner*innen aus diesen Ländern vor dem Datentransfer durch Unterzeichnung eines Vertrags gewährleisten, dass sie die Schweizer Datenschutzregeln einhalten. Umgekehrt kann es der Fall sein, dass in den Ländern der Projektpartner*innen die Datenschutzbestimmungen strenger sind als das in der Schweiz geltende Recht. Dann muss umgekehrt vertraglich vereinbart werden, wie der Datenschutz entsprechend garantiert wird. Der Bund verfügt über eine Liste der Staaten, deren Datenschutzgesetze als dem Schweizerischen ebenbürtig angesehen werden.

Bei Forschungen in Ländern mit unsicheren Netzen sind für den Datentransfer regelmässig Aufenthalte an Orten mit einer stabilen Internetverbindung einzuplanen. Für den Transfer von Forschungsdaten kann SWITCHfilesender genutzt werden. Sensible Daten sollten für den Transfer und die Speicherung stets verschlüsselt werden.

Welche Kommunikationsmittel sind für den Austausch in der Projektgruppe und mit Untersuchungspersonen geeignet?

Es ist darauf zu achten, dass für den projektinternen Austausch und die Kommunikation mit Untersuchungspersonen sichere Kommunikationsmedien gewählt werden, welche den Datenschutz — und dadurch bei heiklen Themen letztlich auch den Schutz der Forschenden und der Untersuchungspersonen — gewährleisten. Facebook, WhatsApp und ähnliches sind also je nach Zusammenhang keine geeigneten Kommunikationsmittel. Für Messenger-Funktionen eignen sich beispielsweise Threema und Signal. Bei den IT-Abteilungen der Universitäten kann abgeklärt werden, welche Webkonferenz-Software sie unterstützen und empfehlen.
In einigen Ländern, wie zum Beispiel China werden manche Kommunikations-Apps, die eine sichere End-to-End-Verschlüsselung enthalten, technisch unterbunden. Forschende sollten sich vor der Arbeit vor Ort informieren, welche Dienste genutzt werden können.

Wie ist mit handschriftlichen Notizen umzugehen?

Grundsätzlich ist der Datenschutz auch bei handschriftlichen Notizen zu beachten. Enthalten diese also personenbezogene Daten, sind die Notizen vertraulich und vor Zugriff unautorisierter Personen zu schützen. Besteht die Gefahr einer Konfiszierung von Forschungsunterlagen bei der Ausreise, muss daran gedacht werden, auch alle analogen personenbezogenen oder heiklen Daten zu digitalisieren und ebenfalls sicher vorab auf einen Heimatserver zu überspielen. Alle handschriftlichen Notizen, die Aufschluss über bestimmte Personen geben, sind zu vernichten. Generell empfiehlt es sich, alle für die Forschung relevanten Daten vor der Ausreise zu digitalisieren und auf einen Server, für den regelmässig ein Back-up erstellt wird, zu überspielen. So beugt man einem Verlust der Daten vor. Bei der Nutzung von SWITCHdrive ist allerdings zu beachten, dass dort kein automatisches Back-up erstellt wird.

Was bedeutet das für diesen Fall?

Die Forschenden haben sich bei der Planung ihres Projekts zu den Textilfabriken bei den zuständigen Stellen ihrer Universität Rat zum Datenaustausch in internationalen Kooperationsprojekten, zur Datensicherheit im Ausland sowie eine Übersicht über die Sicherheitsvorgaben der beteiligten Universitäten geholt. Bei unterschiedlichen Vorgaben der einzelnen Universitäten und Länder halten sie sich an die strengsten Sicherheitsstandards.

Zum Projektbeginn lassen sie sich von jeder Universität ein Projektlaufwerk einrichten, auf den nur die Mitarbeitenden des Projekts Zugriff haben. Sie vereinbaren, wo die Originale gespeichert werden, welche Daten sie hinterher in der Forschungsgruppe miteinander teilen und wie sie dabei vorgehen. Vor ihrer Abreise lassen sie sich bei den IT-Abteilungen ihrer Universitäten beraten und verschlüsseln ihre Rechner. Die IT-Abteilungen haben die Rechner für die Forschenden eingerichtet und geprüft, dass diese aktuelle Patches aufweisen und alle Sicherheitsfeatures angeschaltet sind. Die Projektleitung hat sich darum gekümmert, dass auch die privaten Laptops diesen Sicherheitsstand aufweisen, sofern keine Leih-Geräte der Universität zur Verfügung stehen. Sie hat ebenfalls sichergestellt, dass alle Mitarbeitenden Zugang zum Netzwerk ihrer Universität und zum jeweiligen Projektlaufwerk haben. Wenn die Forschung mit privaten Geräten erfolgt, so haben die betroffenen Mitarbeitenden alle nicht benötigten privaten Daten darauf gelöscht.

Während ihres Forschungsaufenthaltes legen sie private und Forschungsdaten in separaten Verzeichnissen ab. Sie achten darauf, politisch brisante Informationen vorsichtig zu formulieren und verwenden für die Interviewpartner eigene Kürzel und nicht den richtigen Namen. Sie fahren regelmässig in eine grössere Stadt und überspielen die Daten verschlüsselt auf die Server ihrer Heimat-Universitäten. Nach diesen Transfers löschen sie die Daten von ihren Laptops. Vor jeder Ausreise kontrollieren sie, dass alle Daten gelöscht und überschrieben sind.