Datenschutz-Folgenabschätzung für XXX

# German Biobank Alliance ( GBA)-Infrastruktur

Im Rahmen der BMBF-Förderung: „Ertüchtigung deutscher Biobank-Standorte zur Anbindung an BBMRI“ haben sich zunächst elf deutsche Biobankstandorte zur German Biobank Alliance (GBA) unter der Koordination vom German Biobank Node (GBN) zusammengeschlossen. Zur Ermöglichung eines schnellen Auffindens und Zusammenstellens von Biomaterial und Daten für zukünftige nationale und translationale Forschungsprojekte sowie die Anbindung an das europäische Biobanken-Netzwerk BBMRI-ERIC werden modulare und interoperable IT-Komponenten konzipiert, entwickelt und implementiert, die ein standortübergreifendes effizientes Biobanking zulassen. An den beteiligten GBA-Standorten werden Daten aus der klinischen Dokumentation oder aber im Kontext von Forschungsprojekten erhobene Daten mit dort vorhandenen Biomaterialproben verknüpft und über ein lokales Data Warehouse als Bestandteil eines "Brückenkopfes" für verteilte Suchanfragen zur Verfügung gestellt. Die Erhebung und Speicherung der Daten von Patienten/Probanden/Spendern erfolgt nur in der jeweiligen Institution. Rechtsgrundlage ist die informierte Einwilligung, in der der Patient/Proband/Spender auch über sein Recht auf Auskunft und Widerruf aufgeklärt wird (Mustertext AKEK). Diese lokal (d.h. im Brückenkopf) gespeicherten Datensätze können über die dezentrale Suche der GBA angefragt werden.

Ein Brückenkopf besteht aus Hard- und Software-Komponenten und dient dazu, die Daten des jeweiligen Standorts in ein GBA-kompatibles Format zu überführen und für die anderen Komponenten nutzbar zu machen. Die lokal in der Einrichtung der Biobank installierten Softwarekomponenten sind:

* *Lokales Datenmanagement*:

Es stellt die in den lokalen Primärsystemen prinzipiell vorliegenden, aber unterschiedlich strukturierten Datenbestände für eine Nutzung in der GBA bereit. Diese Komponente entspricht funktional und technisch weitgehend einem lokalen Data Warehouse.

* *Teiler*:

Er ist für eine kontrollierte Freigabe der Datenbestände des lokalen Data Warehouse zur Nutzung durch Projekte zuständig.

* *Lokales Identitätsmanagement*:

Es stellt für die Pseudonymisierung von Spendern eine einheitliche Funktionalität bereit.

Da die Komponenten unter der Kontrolle des jeweiligen Standortes stehen, wird sichergestellt, dass die in diesen Komponenten gespeicherten Daten weiter unter der Hoheit der Institution, in der sie erhoben wurden, bleiben. Die Authentifizierung von Benutzern für die Nutzung von lokalen Komponenten obliegt den Standorten selbst.Alle Kommunikationsvorgänge zwischen den Brückenköpfen der Standorte und den zentralen Komponenten werden von den Brückenköpfen initiiert. Für die Anmeldung an den Zentralen Komponenten auf Servern des DKFZ ist eine Authentifizierung notwendig. Der Authentifizierungsdienst bietet eine einheitliche, einmalige Anmeldung („Single Signe On“) sowohl von Nutzern als auch von den Komponenten untereinander.

# GBA-Infrastruktur, umgesetzt am Standort XXX

Spezifische Darstellung der IT-Infrastruktur am eigenen Standort.

**GBA-Brückenkopf**

Der Brückenkopf wird aus CentraXX-Extern gespeist. Die in CentraXX-Extern zur Verfügung stehenden Daten werden vor der Übermittlung an den Brückenkopf auf den von GBA vorgegebenen Datensatz reduziert. Durch diese Dezimierung der Attribute wird das Schutzniveau entsprechend des Erwägungsgrundes 6 und des Artikels 32 der DSGVO im Sinne der Patienten/Probanden/Spender ein weiteres Mal erhöht. Der Zugriff auf die Daten im Brückenkopf erfolgt in Form einer Anfrage (Query) über den GBA-Suchbroker (siehe Abbildung 1). Ein Forscher stellt über den Suchbroker eine Suchanfrage, indem der seine Projektidee beschreibt und die dafür benötigte Patientengruppe anhand bestimmter Suchkriterien charakterisiert. Jeder Teiler fragt kontinuierlich den Suchbroker ab, lädt sich die dort abgelegten Suchkriterien incl. der zugehörigen Projektidee herunter und führt die entsprechende Abfrage gegen das lokale Data Warehouse im Brückenkopf aus. Der Teiler beantwortet die Suchabfrage aber erst, nachdem ein Verantwortlicher am Standort die Datenfreigabe autorisiert hat. Das gefundene Suchergebnis wird dann in einer festgelegten Form z.B. als aggregierte Zahl über den Suchbroker an den Forscher zurück übermittelt. Damit hat der Forscher die Möglichkeit, die gewünschten Biomaterialproben und Daten bei der Biobank, die diese vorrätig hat, direkt anzufordern.

**Diskussion anhand der Leitlinien zur Risikobewertung (Erwägungsgrund 77 der DSGVO):**

**Ausgangslage:**

Mehrfach-Datenhaltung durch weitere Speicherung der bereits in CentraXX gehaltenen Daten im Brückenkopf.

**Risiko:**

Das Risiko ist hoch, dem Datensparsamkeitsgebot nicht zu genügen.

**Festlegung der Verfahren und genehmigten Verhaltensregeln für dessen Eindämmung:**

Der Brückenkopf liegt in der lokalen Verantwortung und Hoheit des Standortes. Daten werden nicht an eine zentrale Datenbank weitergeleitet. An den Brückenkopf werden ausschließlich Daten übermittelt, die auf den von GBA vorgegebenen Datensatz reduziert wurden. Durch diese Dezimierung der Attribute wird das Schutzniveau entsprechend des Erwägungsgrundes 6 und des Artikels 32 der DSGVO im Sinne der Patienten/Probanden/Spender erhöht. Der Zugriff auf die Daten im Brückenkopf erfolgt in Form einer Anfrage (Query) über den GBA-Suchbroker. Der Forscher benötigt für diese Anfrage eine dedizierte passwortgeschützte Zugangsberechtigung für die Anmeldung an den Zentralen Komponenten auf Servern des DKFZ, genehmigt und eingerichtet unter Administration von GBA. Das gefundene Suchergebnis wird in einer festgelegten Form z.B. als aggregierte Zahl über den Suchbroker an den Forscher zurück übermittelt.

Durch diese Erhöhung des Schutzniveaus entsprechend des Erwägungsgrundes 6 und des Artikels 32 der DSGVO im Sinne der Patienten/Probanden/Spender ist davon auszugehen, dass das Risiko der Datensparsamkeit und damit einhergehend das Risiko für die Rechte und Freiheiten natürlicher Personen auf das Möglichste beschränkt werden.