Nutzungsordnung für das *Next Generation Sequencing* – Zentrum West German Genome Center: Produktionsstandort der Heinrich-Heine-Universität Düsseldorf

Inhaltsverzeichnis

Präambel

Aufgrund des § 2 Abs. 2 Satz 1 und des § 16 Abs. 1 Sätze 1 und 2 des Gesetzes über die Hochschulen des Landes Nordrhein- Westfalen (Hochschulgesetz - HG) in der Fassung des Hochschulzukunftsgesetzes vom 16.09.2014 (GV. NRW. S. 547), zuletzt geändert durch Gesetz vom 12. Juli 2019 (GV. NRW Nr. 16 S. 377), erlässt das Rektorat der Heinrich-Heine-Universität Düsseldorf in Ausführung der mit der Rheinischen Friedrich-Wilhelms-Universität Bonn und der Universität zu Köln geschlossenen Kooperationsvereinbarung für ihren Produktionsstandort folgende Nutzungsordnung:

1. Allgemeines

Das *Next Generation Sequencing* (NGS)-Zentrum „West German Genome Center“ (nachstehend: WGGC oder Verbundprojekt) ist eine gemeinsame Kooperation der Universität zu Köln, der Rheinischen Friedrich-Wilhelms-Universität Bonn, der Heinrich-Heine-Universität Düsseldorf, der Universität Duisburg-Essen, der Rheinisch-Westfälischen Technischen Hochschule Aachen, der Universität des Saarlandes, dem Max-Planck-Institut für Pflanzenzüchtungsforschung, dem Bundesinstitut für Arzneimittel und Medizinprodukte sowie dem Deutschen Zentrum für Neurodegenerative Erkrankungen Bonn und wird von der DFG als Verbundprojekt gefördert.

Dabei übernehmen die Universität zu Köln, die Rheinische Friedrich-Wilhelms-Universität Bonn und die Heinrich-Heine-Universität Düsseldorf die Sequenzierarbeiten als Produktionsstandorte.

Die vorliegende Nutzungsordnung des Produktionsstandortes Düsseldorf regelt die Nutzung seiner Ressourcen, den Datenschutz, die Datenweitergabe sowie die Prinzipien zur Berechnung der Entgelte von erbrachten Leistungen.

Aufgabe des Produktionsstandortes Düsseldorf für das WGGC ist die Förderung der Forschung auf dem Gebiet der Genomanalyse vorwiegend unter Verwendung der *long-read*-Sequenziertechnologien von Pacific Biosciences und Oxford Nanopore Technologies.

Der Produktionsstandort Düsseldorf bietet Beratungsleistungen, Analysen und weitere ergänzende Dienstleistungen für Mitarbeiterinnen bzw. Mitarbeiter und Arbeitsgruppen der Heinrich-Heine-Universität und für von der DFG u.A. im Rahmen ihrer Förderinitiative für Hochdurchsatzsequenzierung geförderte Sequenzierprojekte sowie für externe Kooperationspartnerinnen und Kooperationspartner der Universität bzw. für externe Auftraggeber.

Organisation und Struktur des WGGC und der Produktionsstandorte werden durch die Kooperationsvereinbarung für das „West German Genome Center“ zwischen den beteiligten Partnern am Verbundprojekt bzw. durch die Kooperationsvereinbarung zwischen den produktionsstandortbetreibenden Partnern im Rahmen des von der Deutschen Forschungsgemeinschaft (DFG) geförderten „Next Generation Sequenzierungs-Zentrums“ im Rahmen des WGGC geregelt.

2. Leistungen des Produktionsstandortes Düsseldorf

- Qualitätskontrollen der eingehenden RNA und DNA und der eingehenden Zellen, spezielles Vorgehen bei *low-input* Material und hoch molekularen DNA Proben
- Untersuchungen zur Quantität, Qualität und Integrität der Ausgangsproben
- Gegebenenfalls zusätzliche Aufreinigungen des Ausgangsmaterials
- Normalisierung des Ausgangsmaterials
- Vorbehandlungsmaßnahmen des Ausgangsmaterials, z. B. *FFPE repair* für DNA aus fixiertem Material, *dead cell removal* für Zellsuspensionen, Prä-Amplifikation
- Fragmentierung mit verschiedenen Techniken
- Verschiedenste NGS *library*-Präparationsprotokolle für genomische und epigenetische Untersuchungen sowie Transkriptom- und *single-cell*-Transkriptom-Studien
- Amplifikation, Größenselektion und Quantifizierung mittels qPCR
- Sequenzierung mit verschiedenen Readlängen und Sequenziergeräten
- Demultiplexing und Datenqualitätskontrolle
- Weiterführende bioinformatische Analysen

3. Geltungsbereich, Nutzergruppen

Nutzerinnen oder Nutzer des WGGC-Produktionsstandortes Düsseldorf können Personen oder Einrichtungen sein, die aufgrund eines Forschungs- oder Entwicklungsvorhabens begründetes Interesse an der Inanspruchnahme der Infrastruktur oder der Leistungen des WGGC-Produktionsstandortes Düsseldorf haben. Diese Nutzerinnen oder Nutzer werden explizit als „WGGC User“ im Labor-Informations- und Management System des Produktionsstandorts Düsseldorf registriert.

Der WGGC-Produktionsstandort Düsseldorf unterscheidet interne und externe Nutzerinnen oder Nutzer. 50% der DFG finanzierten Gerätekapazität im WGGC sind für DFG-Projekte im Rahmen der DFG Förderinitiative für Hochdurchsatzsequenzierung vorbehalten. Die restlichen 50% der Gerätekapazität können für andere Projekte genutzt werden.

Nutzungsentgelte werden für die internen und für externe Nutzerinnen und Nutzer gemäß Ziffer 7 dieser Ordnung separat festgelegt.

Analysen für externe Nutzerinnen oder Nutzer können im Rahmen einer wissenschaftlichen Zusammenarbeit unter Berücksichtigung der Auslastung des Produktionsstandortes Düsseldorf durchgeführt werden. Bei Überkapazitäten kann der Vorstand des WGGC entscheiden, auch Auftragsanalysen für externe Nutzerinnen oder Nutzer durchzuführen. DFG-geförderte Anfragen haben Vorrang.

Datenschutzrechtlich wird davon ausgegangen, dass es sich grundsätzlich um eine Auftragsverarbeitung gemäß Art. 28 DSGVO (siehe Anlage 1) handelt, sofern nichts anderes zwischen der Nutzerin bzw. dem Nutzer und dem WGGC Produktionsstandort Düsseldorf vereinbart wird.

Diese Nutzungsordnung ist für alle Nutzerinnen und Nutzer des WGGC-Produktionsstandortes Düsseldorf verbindlich.

4. Pflichten der Nutzerin bzw. des Nutzers

Die Nutzerin bzw. der Nutzer garantiert, dass im Fall der Einsendung von Humanproben alle Probanden über die Sequenzierung ihrer Proben und die korrespondierende Datenverarbeitung informiert wurden und ihr/ihm deren schriftliche Einverständniserklärung dazu vorliegt. Diese ist auf Verlangen vorzulegen.

Die Nutzerin bzw. der Nutzer übermittelt dem WGGC-Produktionsstandort Düsseldorf auf Verlangen eine Kopie aller vom Gesetzgeber geforderten Unterlagen und Genehmigungen zum Projekt z.B. das Ethikvotum.

Widerruft ein Proband seine Einwilligung zur Sequenzierung und Verarbeitung seiner genetischen Daten, wird die Nutzerin bzw. der Nutzer unverzüglich den WGGC-Produktionsstandort Düsseldorf darüber informieren. Der WGGC-Produktionsstandort Düsseldorf wird die Daten des betroffenen Probanden dann nicht weiterverarbeiten und von seinen Speichermedien löschen und ggf. noch vorhandenes Probenmaterial vernichten.

Die Nutzerin bzw. der Nutzer stellt sicher, dass Humanproben nur in pseudonymisierter Form an den WGGC-Produktionsstandort Düsseldorf übergeben werden. Die Probenkennung darf keinerlei Rückschlüsse auf die natürliche Person des Probanden erlauben.

5. Prozedere bei Kapazitätsengpässen

Nach den Vorgaben der DFG werden mindestens 50 % der Kapazitäten der im Rahmen dieses Antrags geförderten Sequenziergeräte für DFG-Projekte reserviert.

Der WGGC-Produktionsstandort Düsseldorf meldet dem WGGC Vorstand, wenn ein Kapazitätsengpass vorliegt. Der WGGC Vorstand kann daraufhin den WGGC-Produktionsstandort identifizieren, der genügend Kapazitäten zur Bearbeitung des Projekts oder Teilen daraus hat. In diesem Fall beauftragt der WGGC Vorstand den Nutzer, das Projekt oder die betreffenden Teile des Projektes an den entsprechenden WGGC Produktionsstandort weiterzuleiten.

6. Datenverarbeitung / -speicherung, Ergebnisrückgabe, Datenlöschung, Ende der Verantwortlichkeit

Die nachfolgend ausgeführten Prozesse am WGGC Produktionsstandort Düsseldorf sind in der Anlage 2 (Technische und Organisatorische Maßnahmen) zu dieser Nutzungsordnung, die Bestandteil der Nutzungsordnung ist, dokumentiert.

6.1 Art und Umfang der Datenverarbeitung

Die Datenverarbeitung am WGGC Produktionsstandort Düsseldorf erfolgt ausschließlich für das der Nutzerin bzw. vom Nutzer definierte Projekt mit den zur Erreichung des dort formulierten Forschungsziels erforderlichen und mit der Nutzerin bzw. dem Nutzer vereinbarten Methoden. Der WGGC Produktionsstandort Düsseldorf verarbeitet die Daten nicht zu eigenen Forschungszwecken; grundsätzlich erfolgt die Verarbeitung gemäß Art. 28 DSGVO als Auftragsverarbeitung, es sein denn, mit der Nutzerin dem Nutzer wird vorab eine andre Vereinbarung getroffen. Anonyme Statistiken werden lediglich zu Zwecken der Dokumentation und Qualitätskontrolle genutzt.

6.2 Übermittlung der Daten von der Nutzerin bzw. dem Nutzer an den WGGC Produktionsstandort Düsseldorf

Die Nutzerin bzw. der Nutzer reicht ihre bzw. seine mit nichtsprechenden Pseudonymen versehenen Bio-Proben am WGGC Produktionsstandort Düsseldorf ein. Dort werden sie im Labor verarbeitet und auf den vom WGGC Produktionsstandort Düsseldorf betriebenen Sequenziergeräten sequenziert.

6.3 Ort der Datenverarbeitung und -speicherung

Die Datenverarbeitung erfolgt ausschließlich auf Geräten, Servern und Speichermedien, die vom WGGC Produktionsstandort Düsseldorf (hier: Genomics & Transcriptomics Labor (GTL) oder vom Zentrum für Informations- und Medientechnologie (ZIM)) betrieben und administriert werden. Eine Übermittlung an europäisch sichere Clouddienste ist in besonderen Fällen möglich. Die Daten werden nur von autorisierten Mitarbeiterinnen und Mitarbeitern des GTL verarbeitet. Am ZIM sind nur autorisierte Mitarbeiterinnen und Mitarbeiter mit dem Betrieb und der Administration der Geräte, Server und Speichermedien betraut.

6.4 Übermittlung der Daten und Ergebnisse an die Nutzerin bzw. den Nutzer

Die Ergebnisse aus den vereinbarten Analysen werden der Nutzerin bzw. dem Nutzer übermittelt. Dies kann auf zwei Wegen geschehen:

6.4.1. Datenauslieferung

Die Daten werden in einem passwortgeschützten Bereich gespeichert, auf den die Nutzerin bzw. der Nutzer per Login (Benutzername und Passwort) Zugriff erhält. Die Datenübertragung erfolgt verschlüsselt (SFTP).

6.4.2. Bereitstellung über sichere europäische Cloud Dienste

Ist eine Bereitstellung der Ergebnisse und Daten über einen Cloud Dienst vereinbart, werden die Daten verschlüsselt transferiert und gespeichert. Die Nutzerin bzw. der Nutzer erhält Zugriff auf die Daten über ein persönliches Login mit Benutzername und Passwort. Der Download von Daten durch die Nutzerin bzw. der Nutzer erfolgt ebenfalls verschlüsselt (HTTPS).

6.5 Speicherdauer

Der WGGC-Produktionsstandort Düsseldorf übermittelt Ergebnisse aus der vereinbarten Sequenzierung und Verarbeitung an die Nutzerin bzw. den Nutzer. Übermittelte Daten werden von dem WGGC-Produktionsstandort Düsseldorf laut Löschkonzept (Anlage 3) nach Projektende von den

Speichermedien des WGGC-Produktionsstandortes Düsseldorf gelöscht. Eine physische Löschung der Daten kann aufgrund technischer Bedingungen erst verzögert erfolgen. Näheres ist im Löschkonzept des Produktionsstandortes beschrieben (Anlage 3).

6.6 Verfahren bei Auskunfts-, Löschungs- und Übertragungsanfragen (Art 15, 17, 20 DSGVO)

Die Nutzerin bzw. der Nutzer ist verpflichtet, bei ihr bzw. ihm eingehende Auskunfts-, Löschungs- und Übertragungsanfragen nach Art.15, 17, 20 DSGVO von Probanden dem WGGC-Produktionsstandort Düsseldorf schriftlich mitzuteilen und für die Bearbeitung dieser Anfragen dem WGGC-Produktionsstandort Düsseldorf das Pseudonym des betroffenen Probanden zu benennen.
Der WGGC-Produktionsstandort Düsseldorf wird dann der Löschung nachkommen, siehe Löschkonzept (Anlage 3), bzw. die Daten zwecks Auskunftserteilung oder Übertragung übermitteln.
Auskunfts-, Löschungs- oder Übertragungsanfragen eines Probanden gemäß Art 15, 17, 20 DSGVO, die direkt bei dem WGGC-Produktionsstandort Düsseldorf eingehen, werden an die Nutzerin bzw. den Nutzer zur Prüfung und weiteren Abwicklung übermittelt.

6.7 Ende der Verantwortlichkeit

Der WGGC-Produktionsstandort Düsseldorf ist nur so lange für die Sicherheit und den Schutz der Daten aus dem Projekt verantwortlich, solange die Daten bei dem WGGC-Produktionsstandort Düsseldorf gespeichert sind oder verarbeitet werden.

7. Kosten und Abrechnung

Die Leistungen des WGGC-Produktionsstandortes Düsseldorf sind entgeltpflichtig.

Für die im Rahmen der DFG Förderinitiative für Hochdurchsatzsequenzierung geförderten Projekte werden spezielle, von der DFG bestätigte und direkt bereitgestellte Nutzungsentgelte festgelegt. Für DFG Projekte außerhalb dieser speziellen NGS Förderinitiative wird momentan zusätzlich zu den projektbezogenen Kosten der jeweiligen Untersuchung in der Regel ein Overhead von 22% erhoben.

Für WGGC interne Nutzerinnen und Nutzer werden die anfallenden projektbezogenen Kosten der jeweiligen Untersuchung in Rechnung gestellt. Sollte sich aufgrund einer Bewertung der Finanzbehörden zu einem späteren Zeitpunkt herausstellen, dass auch diese Umsätze einer Steuerpflicht unterliegen, so behält sich der Produktionsstandort vor, nachträglich eine entsprechende Steuer in Rechnung zu stellen.

Für WGGC externe Nutzerinnen und Nutzer werden marktübliche Entgelte inklusive Overhead zuzüglich der gesetzlichen Umsatzsteuer in Rechnung gestellt.

8. Mitwirkung an Veröffentlichungen

Die Nutzerinnen oder Nutzer verpflichten sich, dem WGGC-Produktionsstandort Düsseldorf die Veröffentlichung von Daten, die mit Hilfe des WGGC-Produktionsstandortes generiert wurden, mitzuteilen.

Bei wissenschaftlichen Publikationen ist das Mitwirken des WGGC-Produktionsstandortes Düsseldorf in die Acknowledgements aufzunehmen.

Wurden seitens der Mitarbeiterinnen und Mitarbeiter des WGGC-Produktionsstandortes Düsseldorf wesentliche wissenschaftliche Leistungen in das Projekt eingebracht, ist eine Ko-Autorenschaft der Mitarbeiterinnen und Mitarbeiter aus daraus entstehenden Publikationen gemäß den jeweils gültigen Regeln zur Sicherung guter wissenschaftlicher Praxis der DFG zu prüfen.

9. Haftung

Die Mitarbeiterinnen und Mitarbeiter des WGGC-Produktionsstandortes Düsseldorf können nicht für das Zustandekommen von irrelevanten Daten verantwortlich gemacht werden.
Der WGGC-Produktionsstandort Düsseldorf behandelt Proben mit der gebotenen Sorgfalt. Für den Verlust oder die Beschädigung von Proben (z.B. wegen Stromausfalls) übernimmt der WGGC-Produktionsstandort Düsseldorf keine Haftung.

10. Sonstige Regelungen und Inkrafttreten

Anlagen und damit Bestandteil dieser Nutzungsordnung sind:

- Anlage 1 Mustervertrag über die Auftragsverarbeitung personenbezogener Daten
- Anlage 2 Technische und Organisatorische Maßnahmen für den WGGC Produktionsstandort Düsseldorf
- Anlage 3 Löschkonzept für den WGGC Produktionsstandort Düsseldorf (GTL und ZIM)

Die Nutzungsordnung gilt ausschließlich in Verbindung mit der zugrunde liegenden Kooperationsvereinbarung der produktionsstandortbetreibenden Partner für die Dauer des Vorhabens WGGC. Sie tritt zum 15.05.2021 in Kraft und ersetzt die zum 01.01.2019 in Kraft getretene Nutzungsordnung. Die Nutzungsordnung ist für alle Nutzer des WGGC verbindlich.

Anlage 1 Mustervertrag über die Auftragsverarbeitung personenbezogener Daten

zwischen

[EINFÜGUNG]

vertreten durch [EINFÜGUNG]

– nachfolgend **Auftraggeber** genannt –

und

Heinrich-Heine-Universität Düsseldorf

Universitätsstrasse 1

40225 Düsseldorf

vertreten durch

Genomics and Transcriptomics Laborarory

Prof. Dr. Karl Köhrer

Geb. 22.07.U1

Universitätsstr. 1, 40225 Düsseldorf

– nachfolgend **Auftragnehmer** genannt –

i.S.d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO).

Präambel

Diese Vereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der Nutzungsordnung für das Next Generation Sequencing – Zentrum West German Genome Center: Produktionsstandort der Heinrich-Heine-Universität Düsseldorf, in kraft getreten am 21. August 2020 (nachfolgend „Hauptvertrag“) in ihren Einzelheiten beschriebenen Auftragsverarbeitungen ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen der Auftragnehmer oder durch den Auftragnehmer beauftragte Dritte (Subunternehmer) personenbezogene Daten (»Daten«) im Auftrag des Auftraggebers verarbeiten.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Gegenstand des Auftrages, Art und Zweck der Verarbeitung sowie eine Liste der betroffenen Datenkategorien und Personengruppen ergeben sich aus Anlage 1A zu dieser Vereinbarung.

§ 2 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die in der Anlage 1A konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DS-GVO). Die Verantwortlichkeit des Auftragsnehmers für eigene Pflichten aus den anwendbaren Gesetzen oder aus dieser Vereinbarung bleibt hiervon unberührt.

(2) Die Weisungen werden anfänglich durch den Hauptvertrag sowie diese Vereinbarung

festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt, konkretisiert oder ersetzt werden (Einzelweisung).

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des erteilten Auftrages und der Weisungen des Auftraggebers verarbeiten, außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor. Soweit gesetzlich zulässig, wird der Auftragnehmer den Auftraggeber unverzüglich über das Vorliegen eines solchen Ausnahmefalles informieren.

(2) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

(3) Weisungsberechtigte Ansprechpartnerin des Auftragnehmers ist Dr. Ursula Hilgers, Datenschutzbeauftragte der Heinrich-Heine-Universität Düsseldorf. Sie ist erreichbar unter Datenschutzbeauftragter@uni-duesseldorf.de.

(4) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen des Art. 32 DS-GVO genügen. Er dokumentiert dies für den Zeitpunkt des Abschlusses dieser Vereinbarung in der beigefügten Anlage 2 der Nutzungsordnung. Sofern eine Überprüfung des Auftraggebers einen Anpassungsbedarf der getroffenen technischen und organisatorischen Maßnahmen ergibt, ist dieser zeitnah durch den Auftragnehmer umzusetzen.

(5) Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das gesetzlich vorgeschriebene bzw. zwischen den Parteien vereinbarte Schutzniveau nicht unterschritten wird. Über wesentliche Änderungen der getroffenen Sicherheitsmaßnahmen wird der Auftragnehmer den Auftraggeber schriftlich informieren.

(6) Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 33 bis 36 DS-GVO genannten Pflichten.

(7) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen und darüber hinaus über den ordnungsgemäßen Umgang mit Daten unterrichtet wurden. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

(8) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten (Art. 4 Nr. 12 DS-GVO) des Auftraggebers bekannt werden. Im Falle einer solchen Verletzung trifft der Auftragnehmer unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten, um nachteilige Folgen für die betroffenen Personen bestmöglich zu verhindern. Er wird sich hierfür unverzüglich mit dem Auftraggeber abstimmen.

(9) Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen (ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen).

(10) Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine

datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Hauptvertrag bereits vereinbart.

(11) In besonderen, im Hauptvertrag beschriebenen Fällen bzw. auf Weisung des Auftraggebers, erfolgt eine Aufbewahrung bzw. Übergabe der Daten. Die Bedingungen können gesondert vereinbart werden, soweit der Hauptvertrag hier nicht bereits Regelungen vorsieht.

(12) Daten, Datenträger sowie sämtliche sonstige Materialien sind – sofern nicht anders vereinbart – nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen.

(13) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches zu unterstützen.

(14) Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf Daten des Auftraggebers beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung von Daten ermittelt.

(15) Hat der Auftraggeber eine Datenschutzfolgenabschätzung nach Art. 35 DS-GVO vorzunehmen, so wird er seitens des Auftragnehmers entsprechend unterstützt. Als Unterstützungsmaßnahme leitet der Auftragnehmer dem Auftraggeber insbesondere alle ihm zur Verfügung stehenden Informationen weiter, die zur Datenschutzfolgenabschätzung nach Art. 35 DS-GVO erforderlich sind und unterstützt den Auftraggeber bei einer gegebenenfalls erforderlichen Konsultation der zuständigen Aufsichtsbehörde.

(16) Der Auftragnehmer benennt dem Auftraggeber seinen Datenschutzbeauftragten in §3 (3). Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich in Textform anzuzeigen. Ist die Benennung eines Datenschutzbeauftragen gesetzlich nicht vorgeschrieben, so vermerkt der Auftragnehmer dies. Er sichert insofern zu, dies abschließend geprüft zu haben.

§ 4 Pflichten des Auftraggebers

(17) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(18) Im Falle einer Inanspruchnahme des Auftragnehmers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftraggeber den Auftragnehmer bei der Abwehr des Anspruches zu unterstützen.

(19) Der Auftraggeber nennt dem Auftragnehmer seine weisungsberechtigten Ansprechpartner für im Rahmen des Hauptvertrages oder dieser Vereinbarung anfallende Datenschutzfragen.

§ 5 Anfragen betroffener Personen

(20) Wendet sich eine betroffene Person mit Forderungen zur Geltendmachung ihrer datenschutzrechtlichen Betroffenenrechte unmittelbar an den Auftragnehmer, wird der Auftragnehmer die betroffene Person unverzüglich an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen der Bearbeitung des jeweiligen Antrages der betroffenen Person.

(21) Der Auftragnehmer haftet gegenüber dem Auftraggeber nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird, sofern er die Anfrage entsprechend dieser Vereinbarung vollständig und unverzüglich

weitergeleitet hat.

§ 6 Nachweismöglichkeiten

(22) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach.

(23) Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer werden zu den üblichen Geschäftszeiten und soweit möglich, ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. In dringenden Fällen kann eine vorherige Anmeldung ausnahmsweise entfallen. Der Auftragnehmer darf die Inspektion von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht. Eine Vergütung für die Vorbereitung und Durchführung der Inspektionen wird an den Auftragnehmer nicht gezahlt.

§ 7 Laufzeit

(24) Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit bzw. dem Bestehen des Hauptvertrages. Wird der Hauptvertrag beendet, gilt dies gleichsam für diese Vereinbarung.

(25) Diese Vereinbarung ist unabhängig vom Hauptvertrag nur dann kündbar, wenn der Hauptvertrag auch andere Leistungen umfasst und der Teil, der die Datenverarbeitung im Auftrag zum Gegenstand hat, beendet werden soll. In diesem Falle bedarf es auch einer entsprechenden Anpassung des Hauptvertrages. Für diesen Fall gilt eine Kündigungsfrist von drei (3) Monaten zum Monatsende.

(26) Die Möglichkeit zur fristlosen Kündigung aus einem wichtigen Grund bleibt hiervon unberührt. Ein wichtiger Grund liegt insbesondere vor, wenn eine Pflicht aus dieser Vereinbarung oder Bestimmungen der DS-GVO vorsätzlich oder grob fahrlässig verletzt werden.

(27) Die in dieser Vereinbarung dargelegten Verschwiegenheitsverpflichtungen gelten jedoch auch über den Zeitraum der Kündigung fort.

§ 8 Subunternehmer (weitere Auftragsverarbeiter)

(28) Der Einsatz von Subunternehmern als weiteren Auftragsverarbeitern ist im Rahmen der nachfolgenden Bestimmungen zulässig.

(29) Ein in diesem Sinne relevantes Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der Ganzen oder einer Teilleistung der im Hauptvertrag vereinbarten Leistung beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz und Informationssicherheitsmaßnahmen zu gewährleisten, die das in dieser Vereinbarung vereinbarte Schutzniveau sowie die weiteren datenschutzrechtlichen Vereinbarungen entsprechend abbilden.

(30) Die vertraglich vereinbarten Leistungen oder Teilleistungen werden unter Einschaltung der in Anlage 1B aufgeführten Subunternehmer erbracht.

(31) Vor Hinzuziehung oder Ersetzung der Subunternehmer informiert der Auftragnehmer den Auftraggeber hierüber. Der Auftraggeber kann der Hinzuziehung oder Ersetzung innerhalb einer zweiwöchigen Frist gegenüber der vom Auftragnehmer benannten weisungsberechtigten Person widersprechen. Der Auftraggeber hat hierbei die Gründe anzugeben, welche einer Hinzuziehung oder Ersetzung entgegenstehen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung als erteilt. Liegt ein wichtiger Grund vor, und sofern eine einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich ist, wird dem Auftraggeber ein Sonderkündigungsrecht eingeräumt.

(32) Beabsichtigt der Auftragnehmer die Hinzuziehung von Subunternehmern, welche eine Übermittlung der Daten in ein Drittland i.S.d. Art. 44 DS-GVO beabsichtigt, so hat der Auftragnehmer sicherzustellen, dass die Anforderungen der Art. 44 bis 50 DS-GVO von dem jeweiligen Subunternehmer eingehalten werden. Ferner hat der Auftragnehmer den Auftraggeber hierauf ausdrücklich hinzuweisen.

(33) Nicht als Subunternehmerverhältnisse i.S.d. Absätze sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen oder Bewachungsdienste. Der Auftragnehmer ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz von Daten zu gewährleisten. Die Wartung und Pflege von IT-Systemen oder Applikationen stellt ein zustimmungspflichtiges Unterauftragsverhältnis und Auftragsverarbeitung i.S.d. Art. 28 DSGVO dar, wenn die Wartung und Prüfung solche IT-Systeme betrifft, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden und bei der Wartung auf Daten zugegriffen werden kann, die im Auftrag des Auftraggebers verarbeitet werden.

(34) Der Auftragnehmer ist gegenüber dem Auftraggeber für die Einhaltung sämtlicher Verpflichtungen durch den Subunternehmer verantwortlich. Die Genehmigung des Subunternehmers durch den Auftraggeber befreit den Auftragnehmer nicht von dieser Verpflichtung.

§ 9 Haftung und Schadensersatz

Der Auftragnehmer stellt den Auftraggeber von Schadensersatzansprüchen frei, die die betroffene Person entsprechend Art. 82 DS-GVO gegen den Auftraggeber richtet, soweit die Schadensersatzansprüche aufgrund einer Pflichtverletzung des Auftragnehmers entstanden sind. Im Übrigen gelten die gesetzlichen Regelungen, insbesondere aus Art. 82 DS-GVO.

§ 10 Informationspflichten, Schriftformklausel, Rechtswahl

(35) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und – soweit einschlägig – das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher « im Sinne der DS-GVO liegen.

(36) Änderungen und Ergänzungen dieses Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang von Individualabreden bleibt hiervon unberührt.

(37) Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung zum Datenschutz den Regelungen des Hauptvertrages vor.

(38) Sollte eine Bestimmung dieser Vereinbarung ungültig sein oder werden, so berührt dies die Gültigkeit der übrigen Bestimmungen nicht. Auftraggeber und Auftragnehmer sind insoweit verpflichtet, die ungültige Bestimmung einvernehmlich durch eine Regelung zu ersetzen, die rechtlich zulässig ist und in ihrem wirtschaftlichen Gehalt der ursprünglichen Bestimmung am nächsten kommt.

Entsprechendes gilt für eine Regelungslücke und für den Fall, dass sich eine Bestimmung als aus praktischen oder wirtschaftlichen Gründen undurchführbar oder nicht sinnvoll erweisen sollte.

(39) Es gilt deutsches Recht.

(40) Die beigefügten Anlage 1A und 1B sind Gegenstand dieser Vereinbarung und deren unmittelbarer Bestandteil.

1) Unterschriften

Ort, Datum	Vorname Nachname Auftraggeber	Stempel
Ort, Datum	Vorname Nachname Auftraggeber	Stempel
Ort, Datum	Vorname Nachname Auftragnehmer	Stempel

Anlage 1A Gegenstand des Auftrages

a. Gegenstand des Auftrages; [Beschreibung der Kategorien betroffener Daten sowie die konkreten Zwecke der Verarbeitung der personenbezogenen Daten im Einzelfall]
b. Art und Zweck der betroffenen Datenverarbeitungen sowie Kategorien der Daten und der hiervon betroffenen Personen

Die Verarbeitung umfasst im Einzelnen folgendes:
(Entsprechendes bitte ankreuzen)

	Art der Daten/ Datenkategorien	Kreis der betroffenen Personen (z.B.: Kunden, Teilnehmer Klinische Studien, Mitarbeiter, Ärzte, Geschäfts-partner)	Zweck der Datenverarbeitung dieser Daten
☐	Daten zur Gesundheit (z.B. genomische DNA, RNA, einschließlich Gewebe-, Blutproben)		Auswertungszwecke, For-schungszwecke
☐	Metadaten zur Gesundheit:		Auswertungs- und Forschungs-zwecke
☐			

Anlage 1B Subunternehmer

Der Auftragnehmer setzt zum Zeitpunkt des Abschlusses der Vereinbarung die folgenden Subunternehmer ein:

Unternehmensbezeichnung und Verantwortlicher des Subunter-nehmers	Ausgeführte Leistungen	Beabsichtigte oder Notwendige Daten-verarbeitung in einem Drittland nebst Rechtsgrundlage

Bei beabsichtigtem Drittlandtransfer*: (folgenden Absatz für jeden Unterauftragnehmer mit beabsichtigtem Drittlandtransfer ausfüllen)*

Das angemessene Schutzniveau in _____ist festgestellt durch

☐ einen Angemessenheitsbeschluss der Kommission gemäß Art. 45 Abs. 3 EU-DSGVO;
☐ wird hergestellt durch verbindliche interne Datenschutzvorschriften gemäß Art. 46 Abs. 2 lit. b i.V.m. Art. 47 EU-DSGVO;

- ☐ wird hergestellt durch Standarddatenschutzklauseln gemäß Art. 46 Abs. 2 lit. c und d EU-DSGV);
- ☐ wird hergestellt durch genehmigte Verhaltensregeln gemäß Art 46 Abs. 2 lit. e i.V.m. Art. 40 EU-DSGVO;
- ☐ wird hergestellt durch einen genehmigten Zertifizierungsmechanismus gemäß Art. 46 Abs. 2 lit. f i.V.m. Art. 42 EU-DSGVO;
- ☐ wird hergestellt durch sonstige Maßnahmen gemäß Art. 46 Abs. 2 lit. a, Abs. 3 litt. a und b EU-DSGVO: _____

Anlage 2 Dokumentation der technischen und organisatorischen Maßnahmen für den Produktionsstandort Düsseldorf (IT und Labor)

Stand: 16.06.2020

1. Zutrittskontrolle

Definition zutrittsberechtigter Personen	ja
Regelungen für Fremdpersonal	ja
Chipkarten/Transpondersysteme	ja
Schlüsselregelung	ja
Sicherheitsschlösser	ja
Alarmanlage	wo notwendig
Verschiedene Schließsysteme	wo notwendig
Automatisches Zugangskontrollsystem	wo notwendig
Absicherung der Gebäudeschächte	wo notwendig
Videoüberwachung der Eingänge	wo notwendig
Schließkonzepte	ja
Protokollierung	wo notwendig
Besucherregelung	ja
Berechtigungskonzepte	ja
Dienstanweisung	ja

2. Zugriffskontrolle

Verwalten von Benutzerberechtigungen	ja
Berechtigungskonzepte	ja
Erstellen von Benutzerprofilen	wo notwendig
Login mit Benutzername + Passwort	ja
Definierte Anforderungen an Passwort	ja
Zentrale Passwortvergabe	wo notwendig
Einsatz von Firewalls	ja
Anti-Malware-Systeme	ja
Nutzung von Virtual Local Area Networks	ja
DMZ	wo notwendig
Einsatz VPN bei Remote-Zugriffen	wo notwendig
Datenschutzbelehrung des berechtigten Personals	ja
Dienstanweisung	ja
Aktenvernichtung	ja
Physische Löschung von Datenträgern und Probenmaterial	wo notwendig
Protokollierung der Zugriffe	wo notwendig
Minimale Anzahl an Administratoren	wo notwendig
Datenschutztresor	wo notwendig
Schnittstellenüberwachung/-schutz	wo notwendig
Verschlüsselung von mobilen Endgeräten	wo notwendig
Automatisches Sperren bei Inaktivität und passwortgestützte Aufhebung	wo notwendig

3. Trennungskontrolle

Trennung von Produktiv- und Testumgebung	ja
Physikalische Trennung (Systeme / Datenbanken / Datenträger)	wo notwendig
Logische Trennung (Systeme / Datenbanken / Datenträger)	wo notwendig
Mandantenfähigkeit relevanter Anwendungen	wo notwendig
Trennung Pseudonym-Zuordnungsmerkmal	wo notwendig
Steuerung über Berechtigungskonzept	wo notwendig
Festlegung von Datenbankrechten	ja

4. Pseudonymisierung

Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesicherten System (mögl. verschlüsselt)	wo notwendig

5. Weitergabekontrolle

Email-Verschlüsselung	wo notwendig
Einsatz von VPN	wo notwendig
Datenauslieferung über verschlüsselte Verbindungen wie sftp, tls, …	ja
Nutzung von sicheren/gültigen SSL-Zertifikaten	ja
Nutzung von Fernwartung (Firmen, Beschäftigte)	wo notwendig
Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen	ja
Weitergabe in anonymisierter und pseudonymisierter Form	wo notwendig
Persönliche Übergabe mit Protokoll	wo notwendig

6. Eingabekontrolle

Geschäftsverteilungsplan	wo notwendig
Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	wo notwendig
Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts	wo notwendig

7. Verfügbarkeitskontrolle

Feuer- und Rauchmeldeanlagen	wo notwendig
Feuerlöscher Serverraum	ja
Feuchtigkeitsüberwachung Serverraum	ja
Temperaturüberwachung Serverraum	ja
Schutzsteckdosenleisten Serverraum	ja
Regelmäßige Datensicherung	wo notwendig
Videoüberwachung Serverraum	ja
Alarmmeldung bei unberechtigtem Zutritt zu Serverraum	ja
Räumlich getrennte Aufbewahrung von Sicherungsdatenträgern	wo notwendig
Backup & Recovery-Konzept (ausformuliert)	wo notwendig
Notfallplan	wo notwendig
Durchführung von Notfall- / Wiederanlauftests	wo notwendig
Netzwerküberwachung	wo notwendig
Sicherstellung einer unterbrechungsfreien Stromversorgung (USV)	wo notwendig
Automatische Aktualisierung der Virenscanner auf den Clients	wo notwendig
Virenschutzprogramme sind immer auf dem neuesten Stand	wo notwendig
Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums	ja
Getrennte Partitionen für Betriebssysteme und Daten	wo notwendig

8. Datenschutz-Management

Interner / externer Datenschutzbeauftragter Name / Firma / Kontaktdaten	ja
Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet …)	ja
Mitarbeiter geschult und auf Vertraulichkeit / Datengeheimnis verpflichtet	ja
Regelmäßige Sensibilisierung der Mitarbeiter; Mindestens jährlich	ja
Interner / Externer Informationssicherheitsbeauftragter Name /Firma / Kontakt	wo notwendig
Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt	ja
Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach	ja
Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden	ja
Anderweitiges dokumentiertes Sicherheitskonzept	wo notwendig

9. Incident-Response-Management

Anderweitiges dokumentiertes Sicherheitskonzept	wo notwendig
Einsatz von Firewall und regelmäßige Aktualisierung	ja
Einsatz von Spam-Filter und regelmäßige Aktualisierung	ja
Einsatz von Virenscanner und regelmäßige Aktualisierung	ja
Intrusion Detection System (IDS)	wo notwendig

Interner / externer Datenschutzbeauftragter Name / Firma / Kontaktdaten	ja
Interner / Externer Informationssicherheitsbeauftragter Name /Firma / Kontakt	ja
Mitarbeiter geschult und auf Vertraulichkeit / Datengeheimnis verpflichtet	ja
Regelmäßige Sensibilisierung der Mitarbeiter; Mindestens jährlich	ja
Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt	ja
Interner / Externer Informationssicherheitsbeauftragter Name /Firma / Kontakt	ja
Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach	ja
Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden	ja
Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Daten-Pannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)	ja
Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen	wo notwendig
Einbindung von _DSB und _ISB in Sicherheitsvorfällen und Datenpannen	ja
Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem	ja
Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen	ja

10. Datenschutzfreundliche Voreinstellungen

Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen	wo notwendig
In der Software sind Löschkonzepte implementiert	wo notwendig
Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	ja

11. Auftragskontrolle (Outsourcing an Dritte)

Vereinbarung von Verträgen zur Auftragsverarbeitung	wo notwendig
Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis	wo notwendig

Die Dokumentation der Webanwendung erfolgt laut APP3.1 Webanwendung nach der Vorlage vom Bundesamt für Sicherheit in der Informationstechnik. Die Dokumentation, Stand 11.05.2020 kann auf Wunsch bereitgestellt werden.

Anlage 3 Löschkonzept für den WGGC Produktionsstandort Düsseldorf, Stand: 03.05.2021

1. Biomaterial

Zur Sequenzierung eingeschicktes Biomaterial wird normalerweise während des Verarbeitungsprozesses vollständig aufgebraucht. Verbleibende Reste des Materials und sämtliche Zwischenprodukte des Ausgangsmaterials, die während der Projektdurchführung entstanden sind, werden 8 Wochen nach Abschluss des Projekts durch das Personal der NGS-Produktionsstandortes ordnungsgemäß dokumentiert entsorgt. Die Rückgabe des eingegangenen Biomaterials erfolgt nur auf Verlangen des Einsenders.

2. Elektronische Daten

Storage-Bereiche
Die Storage-Bereiche des WGGC Standorts Düsseldorf sind auf die beiden Einrichtungen Genomics and Transcriptomics Laboratory (GTL) und Zentrum für Informations- und Medientechnologie (ZIM) der Heinrich-Heine-Universität verteilt.

Es bestehen folgende Storage-Bereiche:

Speicherbereich	**Typ**	**Datentyp**	**Einrichtung**
Festplattenspeicher der Sequenzierer	Shortterm	Sequenzdaten	GTL
Festplattenspeicher des Pufferservers	Shortterm	Sequenzdaten	GTL
Paralleles Filesystem des WGGC HPC-Clusters	Shortterm	Sequenzdaten	ZIM
Speicherbereich Auslieferung	Shortterm	Sequenzdaten	ZIM
LIMS Datenbank	Longterm	Nutzerstammdaten	GTL

Shortterm: maximal 2 Monate
Longterm: 10 Jahre

- **Datenträgervernichtung**

  Standort BMFZ: Nutzung des Entsorgungsdienstes des UKD
  Standort ZIM: An der HHU gibt es eine Entsorgungsrichtlinie. Die Entsorgung der IT-Hardware erfolgt gemäß DIN ISO 69933, Schutzklasse 2, Sicherheitsklasse 3
  Papier wird in vorgeschriebenen Datenschutztonnen entsorgt.

- **Wer führt die Löschung durch**

  Die Löschung von Daten geschieht entweder automatisiert durch das Datenmanagement-System des GTL nach programmierten Regeln oder manuell durch Mitarbeiter des GTL.

- **Dokumentation**

  Die automatisierte Löschung von Daten lässt sich durch die jeweiligen Logfiles nachvollziehen.
  Die Datensätze, die manuell gelöscht werden, werden anhand der Liste ‚Art des Löschvorgangs' von dem Verantwortlichen der IT des BMFZ/GTL und seinem Stellvertreter nach einem dokumentierten Prozess durchgeführt.