Langfassung zu Kapitel 4.10 „Biosecurity in mikrobiologischen und biotechnischen Laboratorien“

Zum sicheren Umgang mit Biostoffen im Sinne eines gesamtheitlichen Ansatzes (Biorisk Management) gehören auch Überlegungen, die sich speziell mit den Fragestellungen der „Biosecurity“ befassen. Im Angelsächsischen wird unter *Biosecurity* der Schutz der Einrichtung vor Verlust, Diebstahl, Ausbringung oder internem und externem Fehlgebrauch, einschließlich terroristischer Anschläge, von Biostoffen und Toxinen verstanden. Davon abgegrenzt geht es bei dem Begriff „Biosafety“ um den Schutz der Beschäftigten und der Umwelt vor gefährlichen Biostoffen und Toxinen. Um dies zu gewährleisten, müssen die Sicherheitsmaßnahmen der Schutz- und Sicherheitsstufen und die sonstigen Schutzmaßnahmen eingehalten werden. Dies muss durch regelmäßige Kontrollen/Inspektionen überprüft werden.

Die Begriffe „Biosecurity“ und „Biosafety“ umschreiben eigenständige Konzepte, deren Schutzziele sich teilweise überschneiden, z. B. bei der Zugangskontrolle, beim Anlagenschutz und bei der Kompetenz der Mitarbeiter. Sie sind aber auch komplementär, wie bei den Sicherheitsanforderungen hinsichtlich der Verlässlichkeit der Mitarbeiter. Beiden gemeinsam ist die Anforderung, eine Gefährdungsbeurteilung („risk assessment“) durchzuführen. Dabei betont „Biosafety“, dass Expositionen minimiert und dadurch am Arbeitsplatz erworbene Infektionen verhindert werden. „Biosecurity“ hebt dagegen hervor, dass Arbeitsverfahren und Abläufe so gestaltet sein müssen, dass Biostoffe, aber auch sensible Informationen im weitesten Sinne vor unerwünschter Entnahme, Weitergabe und Fehlgebrauch geschützt bleiben. Um dies zu gewährleisten, müssen solche Schutzmaßnahmen eingehalten werden, welche aus der Gefährdungsbeurteilung mit Blick auf die jeweiligen Schutz- und Sicherheitsstufen abgeleitet worden sind. Deren Wirksamkeit ist durch regelmäßige Kontrollen/Inspektionen zu überprüfen und ggf. anzupassen.

Nach dem bisherigen Stand sind insbesondere Biosecurity-Programme für Laboratorien erforderlich, die mit solchen Biostoffen und biogenen Toxinen arbeiten, die beispielsweise in der Anlage zum Kriegswaffenkontrollgesetz (1), der „EU list of high threat pathogens“ (2), der amerikanischen USDA-Liste über „Select Agents and Toxins“ (3), oder der Australia Group „List of Human and Animal Pathogens and Toxins for Export Control“ (4) enthalten sind. Darüber hinaus empfiehlt auch die WHO,

grundsätzlich alle Laboratorien der Schutz-/Sicherheitsstufe 3 und 4 in Biosecurity-Betrachtungen mit einzubeziehen (5).

Gesetzliche Grundlagen für Biosecurity-Anforderungen finden sich im Anhang II der Biostoffverordnung (6) hinsichtlich des kontrollierten Zugangs zu Biostoffen und im Sicherheitsüberprüfungsgesetz (7), was die Zuverlässigkeit des Personals betrifft. Eine Kombination der Prinzipien von Biosafety und Biosecurity wird im CEN Workshop Agreement (CWA) 15793:2011 (8) erreicht. Hier wurden umfassend alle relevanten Biosicherheitsaspekte im Sinne eines Qualitätsmanagements zusammengeführt, um die Effektivität des Gesamtlabormanagements zu steigern.

4.10.1 Erstellung und Entwicklung eines Biosecurity-Programms

Im Rahmen eines Biosecurity-Programms muss analysiert werden, wie mit geeigneten Maßnahmen Verlust, Diebstahl, Zerstörung von Labor- und Vermögenswerten, Freisetzung und beabsichtigtem Fehlgebrauch von gefährlichen Biostoffen vorgebeugt werden kann. Der damit verbundene Aufwand und die entstehenden Kosten sollten aber stets in Relation zum Risiko gesehen werden und letztlich zweckmäßig, verhältnismäßig und somit angemessen sein. Biosecurity-Maßnahmen können nicht vor allen denkbaren Szenarien schützen. Ziel ist dennoch, derartige Risiken zu erkennen, zu definieren und ihrer Bedeutung nach im Maßnahmenkatalog zu priorisieren.

Wesentliche Elemente eines Biosecurity-Programms können dabei sein:

1. Physikalische Sicherheit und Zugangskontrollen einer Einrichtung
2. Inventarisierungsprozesse (Materialmanagement)
3. Feststellung persönlicher Zuverlässigkeit (Personalmanagement)
4. Verfahrensregelungen zum Transport gefährlicher Biostoffe
5. Verfahren zur Sicherung sensibler Informationen (IT-Security)
6. Implementierung einer *Kommission für Ethik sicherheitsrelevanter Forschung* (KEF)
7. Notfallplanung

4.10.1.1 Leitfaden zum Biosecurity Risk Assessment

Grundlegende Hinweise und Verfahren für die Erstellung einer Gefährdungsbeurteilung „Biosecurity“ sind beispielsweise im „Laboratory Biosafety and Biosecurity Risk Assessment Technical Guidance Document“ von Sandia National

Laboratories zu finden (9).

Die Gefährdungsbeurteilung kann in fünf Hauptschritten erfolgen:

I. Identifikation und Bewertung der Biostoffe und Toxine, wertvoller Ausrüstung und Einrichtung, sensibler Informationen, Reagenzien, Labortiere
II. Identifikation und Einschätzung der Bedrohung der Einrichtung durch potenzielle Gegner (finanzieller Schaden, Reputation, wissenschaftliche Auswirkungen u.a.)
III. Risikoanalyse anhand von spezifischen Gefährdungsszenarien (z. B. Diebstahl, Zerstörung, Umweltschaden, patentrechtlicher Missbrauch, ideeller Schaden)
IV. Entwicklung eines Konzepts zu Beherrschung des Gesamtrisikos und Implementierung von adäquaten Schutzmaßnahmen
V. Regelmäßige Überprüfung von identifizierten Risiken sowie der Wirksamkeit getroffener Sicherheitsmaßnahmen

I. Im ersten Schritt muss das gefährliche und dadurch wertvolle biologische Material (die Biostoffe und Toxine) eindeutig identifiziert werden. Es muss festgestellt werden, in welcher Form sie zur Verfügung stehen, wo und in welcher Menge sie gelagert werden. Wenn beispielsweise in analytischen und diagnostischen Laboratorien nur geringe Mengen an Biostoffen und Toxinen behandelt und aufbewahrt werden, können alle weiteren Schritte entfallen.

II. Im zweiten Schritt muss der Frage nachgegangen werden, ob und wie die vorhandenen Biostoffe und Toxine zu einer Bedrohung werden können. Hierbei kann es erforderlich sein, zu prüfen, wie potenzielle Gegner wie konkurrierende Wissenschaftler, Personen in wirtschaftlicher Zwangslage, verärgerte (ehemalige) Beschäftigte, terroristische oder militante Organisationen nicht zuträglich wirken könnten. Derartige Störer können weiter in Personen mit berechtigtem Zugang zum Labor und/oder zur Einrichtung (Insider) und Personen ohne autorisierten Zugang (Außenstehende) eingeteilt werden. Es kann dabei abgestufte Ebenen des Zugangs zu bestimmten Vermögenswerten geben; Einige „Insider“ haben in unterschiedlichem Umfang Zugang zu bestimmten Vermögenswerten. Die Motivationen für derartiges Fehlverhalten kann durchaus unterschiedlich begründet sein:

- Finanzielle Zwänge (auch Suchterkrankungen)
- Zerstörungswille
- Vorsätzliche Beschädigung oder Vernichtung
- Provokation von Unfällen
- Verbreitung von Angst
- Politisch motivierte Handlungen
- Psychische Verstimmungen oder Erkrankungen
- Ärger

III. Im dritten Schritt wird das Risiko mit Hilfe von spezifischen Security-Szenarien unerwünschter Vorkommnisse näher analysiert. Dabei kann dann folgenden Fragen konkreter nachgegangen werden:

- Wer hat Zugang zu gefährlichen Biostoffen, sensiblen Informationen, wertvoller Ausrüstung, Laborexperimenten?
- Wo kann Sabotage stattfinden?
- Was kann im Vorfeld getan werden, um unerwünschte Ereignisse zu vermeiden?
- Wie können Schutzmaßnahmen umgangen werden und wie verletzlich ist das System?

Die Einschätzung dieser Fragen bleibt letztlich eine Wahrscheinlichkeitsaussage und kann als Funktion von Eintrittswahrscheinlichkeit und Schadenshöhe beschrieben werden. In diesem Zusammenhang sollte man zu folgenden Einschätzungen kommen:

- Welche Bedrohungslagen sind möglich und welche sind wahrscheinlich?
- Sind für den Täter Vermögenswerte (und in welcher Höhe) attraktiv?
- Wie groß kann der erwartete Schaden bei Eintritt eines solchen Ereignisses sein?
- Sind die bestehenden Vorsichtsmaßnahmen geeignet und ausreichend, bekannte Bedrohungsszenarien abzuwenden?

Die Analyseergebnisse sollten schriftlich dokumentiert werden. Schließlich sollte die Leitung der Einrichtung darüber ins Bild gesetzt werden, um zu entscheiden, welche Szenarien weiter zu verfolgen sind.

IV. Im vierten Schritt wird ein Programm erstellt, in dem alle gängigen Risiken erfasst sind. Das Management muss anschließend festlegen, welche Szenarien ein inakzeptables Risiko darstellen und welche Risiken mit bereits bestehenden Kontrollen und Schutzmaßnahmen abgedeckt sind. Ein Biosecurity-Plan wird implementiert, der Maßnahmen zur Risikominimierung ausweist und in Schriftform Standardbetriebsanweisungen und Verfahrensweisen bei entsprechenden Vorfällen in Kraft setzt. Außerdem muss das Management die Kosten für die Umsetzung des Planes beziffern und in den Haushalt einkalkulieren.

V. Im fünften Schritt geht es um die regelmäßige Überprüfung der vom Management ursprünglich definierten Biosecurity-Schutzziele. Es muss wiederkehrend festgestellt werden, ob die Risikobewertungen nach wie vor Bestand haben sowie die Gefährdungsbeurteilung überprüft und ggf. fortgeschrieben und das Programm entsprechend aktualisiert geführt und weiterentwickelt werden. In allen Fällen muss das Management sicherstellen, dass das von ihm in Kraft gesetzte Konzept gelebt wird, durch Training eingeübt und durch Überprüfung verifiziert wird. Im Gegensatz zu Biosafety-Maßnahmen sind Biosecurity-Elemente oder -Bestandteile nicht als Mindestanforderung ausgelegt.

4.10.1.2 Implementierung des Biosecurity Programms

Im Rahmen der Implementierung des Biosecurity-Plans ist es erforderlich, einen Verantwortlichen zu benennen sowie die erforderlichen sachlichen, personellen und finanziellen Mittel zur Verfügung zu stellen. Dann ist eine Organisationsstruktur aufzubauen, die in der Lage ist, die Kette der Anweisungen, Aufgaben und Funktionen zu gewährleisten. Eine effiziente Implementierung eines Biosecurity-Programms bedeutet, dass ein Plan aufgestellt, Maßnahmen eingeübt, ggf. modifiziert und anschließend in die Politik und Absichten des Unternehmens integriert wird. Abschließend muss die Wirksamkeit des Biosecurity-Managements anhand von Audits zertifiziert werden. Auf der Grundlage anerkannter Management-Standards, beispielsweise ISO/IEC 17021 und in Verbindung mit dem CWA 15793 bzw. ISO/DIS 35001 „Biorisk management for laboratories and other related organisations", kann eine Eigenkontrolle vorgenommen werden.

4.10.1.3 Biosecurity trifft auf Biosafety

Wie zu Beginn ausgeführt, umschreiben die Begriffe „Biosecurity" und „Biosafety" eigenständige Konzepte, deren Schutzziele sich teilweise überschneiden oder sogar

gegenläufig sein können. So kann die Installation von biometrischen Zugangskontrollen der Zielsetzung von Biosafety entgegenlaufen, wenn z.B. Fingerprint-Scanner an Tiefkühlschränken dazu führen würden, dass das Personal die Schutzhandschuhe im Containment ausziehen müsste, oder auch die Schutzbrillen bei der Installation von Iris-Scannern innerhalb des Containments.

Aus Sicht von Biosafety sollen alle Mitarbeiter im Sicherheitsbereich über die vorhandenen Biostoffe und Pathogene informiert sein, um eine Gefährdung durch Exposition möglichst zu vermeiden. Biosecurity zielt demgegenüber darauf ab, dass nur ein eingeschränkter und klar benannter Personenkreis über die verwendeten und gelagerten Krankheitserreger und Toxine informiert wird.

Anforderungen von Biosafety erfordern, dass der Zugang zum Containment für Notfallsituationen auch mit externen Ersthelfern geübt und trainiert werden muss. Gleichwohl müssen aus Sicht der Biosecurity Verfahrensweisen implementiert sein, dass auch in Notfallsituationen mit Bruch der Containmentgrenzen ein Entwenden oder Missbrauch von relevanten Biostoffen sicher verhindert werden kann.

Es gilt der Grundsatz: Biosecurity-Programme dürfen Laborarbeiten nicht behindern oder gar gefährden. Insoweit ist eine sinnvoll abgestufte Herangehensweise dringend geboten.

4.10.1.4 Umgang mit sicherheitsrelevanter Forschung – Dual use research of concern (DURC)

Im Mai 2014 haben die Deutsche Forschungsgemeinschaft (DFG) und die Deutsche Akademie der Naturforscher Leopoldina ihre Schrift „Wissenschaftsfreiheit und Wissenschaftsverantwortung – Empfehlungen zum Umgang mit sicherheitsrelevanter Forschung“ veröffentlicht (10). Diese Empfehlungen richten sich an alle Wissenschaftsdiziplinen, nicht nur an die Lebenswissenschaften, und zielen auf eine Selbstregulierung/Selbstverpflichtung der Wissenschaft ab.

Kernempfehlungen sind:

1. Beachtung von ethischen Grundsätzen durch den Forschenden über rechtliche Regeln hinaus
2. Risikoanalysen von Forschungsvorhaben
3. Risikominimierung
4. Prüfung von (geplanten) Veröffentlichungen auf Risiken

5. Verzicht auf Forschung als letztes Mittel
6. Dokumentation und Mitteilung von Risiken
7. Schulung, Aufklärung und Bewusstseinsschärfung
8. Klarheit über die verantwortliche Person
9. Verfügbarkeit von Compliance-Stellen
10. Definition von Ethikregeln durch die Forschungsinstitutionen
11. Einrichtung von Kommissionen für Ethik sicherheitsrelevanter Forschung (KEF) an Forschungsinstitutionen

Es ist wünschenswert, dass alle Forschungsinstitutionen für mögliche Biosecurity-Themen und insbesondere für ein „Dual use research of concern“ (DURC) sensibilisiert werden, Ethikregeln definieren und spezielle Kommissionen für Ethik der Forschung (KEF) bilden, die in Fragen der sicherheitsrelevanten Forschung beraten und sicherheitsrelevante Forschungsvorhaben beurteilen.

4.10.2 Rechtsgrundlagen zur Regelung von Biosecurity

4.10.2.1 Biostoffverordnung

Die Biostoffverordnung (BioStoffV) verlangt zur „**Abwendung von Gefahren“** und bei **„außergewöhnlichen Umständen“** eine planmäßige Vorgehensweise, die darauf ausgerichtet ist, die Exposition der Beschäftigten gegenüber pathogenen Mikroorganismen (Risikogruppe 3 und 4) im Gefahrfall so gering wie möglich zu halten (11). In einem innerbetrieblichen „Gefahrenabwehrplan“ müssen die kurzfristig zu ergreifenden Sicherheitsmaßnahmen vor Aufnahme von Tätigkeiten der Schutzstufe 3 oder 4 dargelegt werden. Dies setzt voraus, dass bereits im Vorfeld die möglichen Umstände untersucht werden, die wahrscheinlich und erfahrungsgemäß im Gefahrenfall auftreten können (§ 13). Zudem lösen Unfälle und Störungen bei Tätigkeiten mit Biostoffen der Risikogruppen 3 und 4, die zu Gesundheitsgefahren, Krankheits- und Todesfällen bei den Beschäftigten führen oder führen können, Informationspflichten des Unternehmers gegenüber der zuständigen Behörde aus (§ 17 Abs. 1). Auf der Basis dieser Informationen kann die zuständige Behörde im Benehmen mit dem Arbeitgeber die erforderlichen Schutzmaßnahmen unverzüglich veranlassen, auch gegenüber Dritten.

4.10.2.2 Gentechnik-Notfallverordnung

Gegenstand der Gentechnik-Notfallverordnung (GenTNotfV) sind Unfälle,

Vorkommnisse und nicht beabsichtigtes Entweichen von gentechnisch veränderten Organismen (GVO), die zu einer Gefahr für die Rechtsgüter nach § 1 Nr. 1 des Gentechnikgesetzes (GenTG) werden können. Zur Vorbereitung auf diese Eventualfälle werden in besonderen Fällen **außerbetriebliche Notfallpläne**, Informationen sowie Organisations- und Sicherheitsmaßnahmen verlangt, die die zuständige Behörde und den Betreiber in die Lage versetzen sollen, im Vorfeld geeignete Maßnahmen zur Beherrschung dieser Ausnahmesituation zu ergreifen. Diese Maßnahmen können teilweise mit denen eines Biosecurity-Programms übereinstimmen oder diese ergänzen.

4.10.2.3 Sicherheitsüberprüfungsgesetz (SÜG)

Das Sicherheitsüberprüfungsgesetz des Bundes (SÜG) wurde novelliert. Die neue Fassung ist seit dem 21. Juni 2017 in Kraft (13). Das SÜG ist insbesondere dann anzuwenden, wenn eine Behörde oder sonstige öffentliche Stelle des Bundes einer Person eine sicherheitsempfindliche Tätigkeit zuweisen möchte oder eine Verschlusssache an eine nicht-öffentliche Stelle weitergeben will. Eine sicherheitsempfindliche Tätigkeit übt insbesondere aus, wer an einer sicherheitsempfindlichen Stelle innerhalb einer lebens- oder verteidigungswichtigen Einrichtung beschäftigt ist oder werden soll (vorbeugender personeller Sabotageschutz). Ziel des vorbeugenden personellen Sabotageschutzes ist es, potenzielle Saboteure (Innentäter) von sicherheitsempfindlichen Stellen fernzuhalten. Nur auf diese Weise kann der Schutz von Gesundheit oder Leben großer Teile der Bevölkerung oder Schutz vor einer Beeinträchtigung oder Beunruhigung des funktionierenden Gemeinwesens sichergestellt werden. Die die Bundesrepublik Deutschland bildenden Länder haben jeweils für ihre Landesbehörden entsprechende Gesetze erlassen, die im Kern dem SÜG des Bundes entsprechen. Im Sinne des SÜG liegt ein Sicherheitsrisiko vor, wenn tatsächliche Anhaltspunkte Zweifel an der Zuverlässigkeit des Betroffenen bei der Wahrnehmung einer sicherheitsempfindlichen Tätigkeit begründen oder eine besondere Gefährdung durch Anbahnungs- und Werbungsversuche fremder Nachrichtendienste, insbesondere die Besorgnis der Erpressbarkeit, begründen oder Zweifel am Bekenntnis des Betroffenen zur freiheitlichen demokratischen Grundordnung im Sinne des Grundgesetzes oder am jederzeitigen Eintreten für deren Erhaltung begründen. Bei Feststellung eines Sicherheitsrisikos darf die betroffene Person nicht mit einer sicherheitsempfindlichen Tätigkeit betraut werden. Die sicherheitserheblichen Erkenntnisse können sich sowohl

über die zu überprüfende Person als auch den einzubeziehenden Partner (Ehe- oder Lebenspartner) ergeben.

4.10.2.4 Verordnung (EG) Nr. 428/2009 des Rates über eine Gemeinschaftsregelung für die Kontrolle der Ausfuhr, der Verbringung, der Vermittlung und der Durchfuhr von Gütern mit doppeltem Verwendungszweck (Dual-Use-Verordnung)

Die EG-Dual-Use-Verordnung (14) ist als Verordnung der Europäischen Union für die Mitgliedstaaten unmittelbar verbindliches Recht. Regelungsgegenstand ist der Export von Dual-Use-Gütern. Die Ausfuhr solcher Güter in einen Nicht-EU-Staat ist grundsätzlich genehmigungspflichtig. Erfasst sind solche Güter, die sowohl zivilen als auch militärischen Zwecken zugeführt werden können (15). Jedoch sind unabhängig davon alle „Güter“ von der Genehmigungspflicht erfasst, die in Anhang I aufgeführt sind, dabei auch biologisches Material wie zum Beispiel aviäre Influenzaviren. Die Genehmigung der Ausfuhr erfolgt nach einem zweistufigen System: Zunächst ist die Feststellung der Genehmigungspflicht anhand des Anhangs zur Verordnung zu treffen, bevor die Entscheidung über die Genehmigungsfähigkeit erfolgt. Der genehmigungsrelevante Begriff der „Güter mit doppeltem Verwendungszweck“ erfasst auch „Technologie“, also „spezifisches technisches Wissen“, das in technischen Unterlagen verkörpert ist. Demnach können auch Publikationen dem Kontrollregime unterfallen. Allerdings sind in den technischen Güterbeschreibungen des Anhangs Grundlagen, Forschung und allgemein zugängliche oder für die Patentanmeldung erforderliche Informationen von der Genehmigungspflicht generell ausgenommen. Darüber hinaus knüpft die Genehmigungsentscheidung an greifbare Anhaltspunkte für einen Missbrauch des Exportgutes im Sinne einer konkreten Gefahrenlage an. Ein Biosecurity-typisches generelles Missbrauchspotenzial des Gutes reicht somit nicht aus, um eine Genehmigungsversagung zu begründen. Gegenstand der EG-Dual-Use-Verordnung sind im Übrigen nur Fragen der Ausfuhr. Die Entstehung von Risiken im Forschungsprozess selbst und forschungsbezogene Biosecurity-Risiken sind nicht Inhalt des Exportrechts. Neben der EG-Dual-Use-Verordnung sind für das in Deutschland wirksame Exportkontrollrecht insbesondere das Außenwirtschaftsgesetz (AWG) und die Außenwirtschaftsverordnung (AWV) weitere relevante Rechtsgrundlagen, die sich allerdings ausschließlich auf die Ausfuhrkontrolle von Rüstungsgütern beziehen (15).

Literatur/Internetquellen

- http://www.gesetze-im-internet.de/krwaffkontrg/ abgerufen 4.2.20
- http://ec.europa.eu/health/ph_threats/Bioterrorisme/keydo_bio_01_en.pdf,2005 abgerufen 4.2.20
- https://australiagroup.net/de/human_animal_pathogens.html abgerufen 4.2.20
- http://www.who.int/csr/resources/publications/biosafety/WHO_CDS_EPR_2006_6.pdf abgerufen 4.2.20
- https://www.gesetze-im-internet.de/biostoffv_2013/anhang_ii.html abgerufen 4.2.20
- https://www.gesetze-im-internet.de/s_g/BJNR086700994.html abgerufen 4.2.20
- http://www.uab.cat/doc/CWA15793_2011 abgerufen 4.2.20
- http://prod.sandia.gov/techlib/access-control.cgi/2014/1415939r.pdf abgerufen 4.2.20
- http://www.leopoldina.org/uploads/tx_leopublication/2014_06_DFG_Leopoldina_Wissenschaftsfreiheit_-verantwortung_D.pdf, abgerufen am 04.06.2018
- http://www.gesetze-im-internet.de/biostoffv_2013/index.html abgerufen 4.2.20
- http://www.gesetze-im-internet.de/gentnotfv/GenTNotfV.pdf abgerufen 4.2.20
- https://www.gesetze-im-internet.de/s_g/SÜG.pdf abgerufen 4.2.20
- https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:02009R0428-20171216&qid=1542989151165&from=EN abgerufen 4.2.20
- https://www.ethikrat.org/fileadmin/Publikationen/Stellungnahmen/deutsch/stellungnahme-biosicherheit.pdf abgerufen 4.2.20