Datenschutz- und Datensicherheitskonzept am Zentrum für Quantitative Biologie

Fassung vom 24. April 2017

Dr. Sven Nahnsen, Matthias Seybold, Sven Fillinger

Hier kann man einen allgemeinen Einführungstext schreiben, zum Beispiel Motivation, Gesetzgebung und Ziele der Datensicherheitskonzepte am QBiC.

Änderungsnachweis

3. Juli 2014

Author(en): Dr. Sven Nahnsen
Neuerstellung und erste Fassung des Datenschutz- und Datensicherheitskonzepts

24. Juli 2017

Author(en): Dr. Sven Nahnsen, Matthias Seybold, Sven Fillinger
Layout Neuauflage, Aktualisierung von technischen Daten, Überarbeitung der Begriffsabgrenzung `Datenschutz` und `Datensicherheit`.

Inhaltsverzeichnis

Betrieb des Zentrums für Quantitative Biologie (QBiC)

Präambel

Das Quantitative Biology Center (QBiC) wurde 2011 als zentrale Einrichtung der Universität Tübingen und mit Zusammenarbeit der Medizinischen Fakultät Tübingen, sowie dem Max Planck Instituts für Entwicklungsbiologie gegründet. Der technische Betrieb von der QBiC Infrastruktur findet dabei am Zentrum für Datenverarbeitung (ZDV) der Eberhard Karls Universität Tübingen statt.

Dieses Handbuch beschreibt die konkrete Umsetzung der in § 9 Landesdatenschutzgesetz (LDSG) geforderten technischen und organisatorischen Maßnahmen zum Datenschutz bei automatiserter Verarbeitung personenbezogener Daten und zurdas Datensicherheitskonzept am QBiC.

Die nachfolgenden Ausführungen untergliedern sich in Erläuterungen zu datenschutzrechtlichen Begriffen sowie der Definition der Schutzmaßnahmen für die zentrale DV-Anlage, den Netzwerkkomponenten für den Zugang und den lokalen Anschluss.

1 Grundlagen eines Datenschutzkonzeptes gemäß LDSG

Die in diesem Datenschutzkonzept festgeschriebenen Maßnahmen sollen den Missbrauch und die Verfälschung von personenbezogenen Daten verhindern. Werden in öffentlichen Stellen selbst oder im Auftrag Daten dieser Art verarbeitet, so haben die für die Datenverarbeitung (DV) verantwortlichen Stellen gemäß § 9 (3) LDSG in der Fassung vom 2.April 2003 (GBl. S 648) technische und organisatorische Maßnahmen zu treffen, um die Ausführung der Vorschriften dieses Gesetzes zu gewährleisten.
So ist zu gewährleisten, dass

- nur berechtigte Personen auf Datenbestände Zugriff haben (Vertraulichkeit),
- Daten bei der Verarbeitung nicht verfälscht werden (Integrität),
- Datenbestände reproduziert werden können (Verfügbarkeit).

Diese Ziele können erreicht werden durch:

- gebäudetechnische Maßnahmen (gebäudespezifische und räumliche Absicherung),
- hardwaretechnische Maßnahmen (Hardware-Passwortschutz, Schlösser etc.),
- softwaretechnische Maßnahmen (Software-Passwortschutz, Auditing etc.).

Aus o. g. Gesetzestext geht weiter hervor, dass solche Maßnahmen nur erforderlich sind, wenn „[...]der Aufwand, insbesondere unter Berücksichtigung der Art der zu schützenden Daten, in einem angemessenen Verhältnis zum Schutzzweck steht“(siehe LDSG §9 (2)). Es wird daher nachfolgend ein Konzept erarbeitet, welches ausgehend von den am meisten zu schützenden Datenbeständen einen für das gesamte DV System ausreichenden Grundschutz gewährleistet.

1.1 Definition der Maßnahmen gemäß § 9 LDSG

Werden personenbezogene Daten automatisiert verarbeitet, sind Maßnahmen zu treffen, welche die in den folgenden Kapiteln definierten Kontrollvorgaben berücksichtigen.

1.1.1 § 9 (3) Nr. 1 : Zutrittskontrolle

Im Rahmen der Zutrittskontrolle ist Unbefugten der Zugang zu Datenverarbeitungsanlagen zu verwehren. Geeignete Maßnahmen sind dedizierte EDV- und Verteilerräume, verschlossene Diensträume sowie restriktive Schlüsselvergabe.

1.1.2 § 9 (3) Nr. 2 : Datenträgerkontrolle

Die Maßnahmen zur Datenträgerkontrolle sollen verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können.

1.1.3 § 9 (3) Nr. 3 : Speicherkontrolle

Die Speicherkontrolle dient der Vermeidung von unbefugten Eingaben in den Speicher sowie Verhinderung unbefugter Kenntnisnahme, Veränderung oder Löschung gespeicherter Daten.

1.1.4 § 9 (3) Nr. 4 : Benutzerkontrolle

Wird durch technische oder organisatorische Maßnahmen verhindert, dass Datenverarbeitungsanlagen (DVA) mit Hilfe von Einrichtungen zur Datenübertragung unberechtigt genutzt werden, so spricht man von Benutzerkontrolle.

1.1.5 § 9 (3) Nr. 5 : Zugriffskontrolle

Die Zugriffskontrolle gewährleistet, dass die zur Benutzung einer DVA Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.

1.1.6 § 9 (3) Nr. 6 : Übermittlungskontrolle

Ziel der Übermittlungskontrolle ist es, zu gewährleisten, dass überprüft und festgestellt werden kann, an welchen Stellen Daten durch Einrichtungen zur Datenübertragung übermittelt werden können.

1.1.7 § 9 (3) Nr. 7 : Eingabekontrolle

Die Eingabekontrolle stellt sicher, dass nachträglich überprüft und festgestellt werden kann, welche Daten zu welcher Zeit von wem in ein Datenverarbeitungssystem (DVS) eingegeben worden sind.

1.1.8 § 9 (3) Nr. 8 : Auftragskontrolle

Die Auftragskontrolle impliziert, dass eine Verarbeitung von Daten im Auftrag nur entsprechend den Weisungen des Auftraggebers durchgeführt werden kann.

1.1.9 § 9 (3) Nr. 9 : Transportkontrolle

Ziel der Transportkontrolle ist es, zu verhindern, dass sowohl bei der Übertragung als auch während des Transports von Daten auf Datenträgern diese nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können.

1.1.10 § 9 (3) Nr. 10 : Verfügbarkeitskontrolle

Die Verfügbarkeitskontrolle soll gewährleisten, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind.

1.1.11 § 9 (3) Nr. 11 : Organisationskontrolle

Organisationskontrolle bedeutet, dass innerbehördliche und innerbetriebliche Organisationen so zu gestalten sind, dass sie den besonderen Anforderungen des Datenschutzes gerecht werden. Nachfolgend der Maßnahmenkatalog für den Betrieb von QBiC, differenziert nach zentralen Netzwerkkomponenten und Arbeitsstationen.