ANHANG II
Technische und organisatorische Maßnahmen

1. Maßnahmen zur Pseudonymisierung und Verschlüsselung personenbezogener Daten:
Alle personenbezogenen Daten werden ausschließlich in AES-Verschlüsselten MySQL-Tabellen abgespeichert. Zusätzlich werden alle erstellten Datensicherungen mittels AES-Verschlüsselung (RSA-Key) geschützt. Vor einer etwaigen Entsorgung oder Weitergabe von Speichermedien werden alle darauf enthalten Daten physisch gelöscht.

2. Maßnahmen zur fortdauernden Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung:
Die Software wird auf einem Root-Server betrieben, welcher durch die Netcup GmbH bereitgestellt wird. Dabei werden alle Daten auf einem RAID10-Festplattenarray gespeichert. Zur weiteren Vorbeugung von Datenverlust werden zusätzlich alle Daten stündlich auf den Backup- Server am Firmenstandort des Providers übertragen. Eine Sicherung täglich wird für 90 Tage sowie eine Sicherung wöchentlich für die Dauer von 365 Tagen gespeichert. Die Korrektheit und Integrität der Sicherungen wird stichprobenartig durch den Provider geprüft. Alle Mitarbeitenden des Providers werden geschult und auf Vertraulichkeit verpflichtet.

3. Maßnahmen zur Sicherstellung der Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen:
Durch die regelmäßige Datensicherung in Form von MySQL-BULK-Exporten können alle erfassten Daten rasch wiederhergestellt werden. Auch die Wiederherstellung von einzelnen Datensätzen oder Zellen ist dadurch möglich.

4. Maßnahmen zur Identifizierung und Autorisierung der Nutzer:
Zur Identifizierung der NutzerInnen werden Benutzername und Kennwort verwendet. Diese sind nur für die Anmeldung am eigenen Mandat (Schule / Bibliothek) freigeschaltet. Um unerwünschte Zugriffe von Personen ohne Zugangsdaten abzuwenden, wird die Anmeldefunktion nach 10 fehlgeschlagenen Anmeldeversuchen für diesen Client für 30 Minuten gesperrt.

5. Maßnahmen zum Schutz der Daten während der Übermittlung:
Alle Daten werden mittels HTTP sowie mittels Websocket-Protokoll (WS, Erweiterung von HTTP) zwischen Client und Server übertragen. All diese Verbindungen werden mittels HTTPs/WSs verschlüsselt.

6. Maßnahmen zum Schutz der Daten während der Speicherung:
Siehe Punkt 1.

7. Maßnahmen zur Gewährleistung der Protokollierung von Ereignissen:
Alle durchgeführten Aktivitäten (Datenänderungen) werden direkt in der Datenbank gespeichert. Am Server auftretende Fehler (Exceptions, Errors) werden ebenfalls protokolliert und extern abgespeichert.

8. Maßnahmen zur Zertifizierung/Qualitätssicherung von Prozessen und Produkten:

Zur Sicherstellung der Erreichbarkeit des Servers wird alle 15 Minuten automatisiert die Verfügbarkeit aller Dienste geprüft. Beim Auftreten von Fehlern während dieser Prüfung wird der Provider automatisch darüber informiert. Zur Verbesserung der generellen Systemstabilität werden während der Entwicklung Unit- sowie Integration-Tests umgesetzt. Mit diesen wird automatisiert die Funktionalität des abgedeckten Programmteils überprüft. Hiermit wird auch die Konfiguration der Berechtigungen geprüft, um sicherzustellen, dass personenbezogene Daten ausschließlich an Benutzer mit den notwendigen Berechtigungen übermittelt werden. Vor dem Veröffentlichen jeder Systemanpassung werden diese Tests automatisch ausgeführt. Nur nach dem Bestehen dieser Überprüfungen ist das Bereitstellen des Updates möglich. Weiters sind die Datenbank-Systeme für die Entwicklung sowie für den Produktivbetrieb klar abgetrennt.

9. Maßnahmen zur Gewährleistung der Datenminimierung:

Von allen NutzerInnen werden ausschließlich Daten erhoben und gespeichert, welche für den Bibliotheksbetrieb sowie für die notwendigen statistischen Auswertungen (Jahresstatistik, ...) von Nöten sind.

10. Maßnahmen zur Gewährleistung der Datenqualität:

Alle bibliotheksbezogenen Daten werden in einer MySQL-Datenbank gespeichert. Dafür wurde ein passendes Datenbankschema umgesetzt. Dieses Schema, kombiniert mit den automatischen Überprüfungen (Constraints), durch welche beim Erstellen und Bearbeiten von Datensätzen diese automatisch überprüft werden, sichert die Qualität bei der Datenspeicherung. Durch automatische Prüfungen in den Formularen der grafischen Benutzeroberfläche wird der Benutzer bereits beim Verwalten von Daten unterstützt. Auch dadurch wird die Qualität der Daten optimiert.

11. Maßnahmen zur Ermöglichung der Datenübertragbarkeit und zur Gewährleistung der Löschung:

Der Datenexport im CSV-Format ist durch Verwaltungsbenutzer des Bibliotheksteams jederzeit unter Verwaltung > Daten exportieren möglich. Optional kann auf Anfrage des Bibliotheksteams auch ein manueller Datenexport vom Provider erstellt und per E-Mail übermittelt werden. Dabei werden die Daten ausschließlich an die E-Mail-Adresse übermittelt, welche im Zuge der Vertragsübermittlung bekanntgegeben wurde. Um auf Anfrage eines Nutzers alle Daten dieses Nutzers endgültig zu löschen, steht in der Benutzeroberfläche (GUI) beim Leser die Funktion Leserdaten anonymisieren zur Verfügung. Hierbei werden alle Daten des Lesers aus der Datenbank gelöscht. Statistikrelevante Daten (Entlehnungen, ...) werden so anonymisiert, dass diese nur noch dem Medium, der Benutzergruppe / Klasse, der Gebührengruppe sowie dem Wohnort zuzuordnen ist. Die personenbezogenen Daten bleiben in Form von Datensicherungen für weitere 365 Tage am Server gespeichert.