Annex 7c Technical and Organizational Measures

to the Agreement on Commissioned Data Processing (Annex 7a): Technical and Organizational Measures according to Sec. 5 LDSG

ExLibris inter alia employs the following technical and organizational measures to ensure confidentiality, integrity, availability, authenticity, auditability and transparency regarding the processing of personal data:

1 Physical Security

1.1 Ex Libris hardware, network, programs and data ("Ex Libris Systems") are physically secured in the following ways:

1.1.1 Ex Libris Systems are located behind locked steel doors, protected by cardkeys, or biometric devices. Access is restricted to authorized personnel only and anyone seeking access needs to be escorted. Entry to the data center is monitored 24x7.

1.1.2 Ex Libris Systems require key access and are protected by alarm systems and/or video surveillance systems when the location is not manned.

1.2 Ex Libris Systems are environmentally protected using the following:

1.2.1 Ex Libris Systems are housed in a temperature- and humidity-controlled environment; and

1.2.2 Ex Libris Systems are located in a room with fire suppression

Anlage 7c Technische und organisatorische Maßnahmen

zum Vertrag zur Datenverarbeitung im Auftrag (Anlage 7a): technische und organisatorische Maßnahmen entsprechend § 5 LDSG

ExLibris setzt unter anderem die folgenden technischen und organisatorischen Maßnahmen ein, um die Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Nachvollziehbarkeit und Transparenz hinsichtlich der Verarbeitung personenbezogener Daten sicherzustellen:

1 Physische Sicherheit

1.1 Hardware, Netzwerk, Programme und Daten von ExLibris ("Ex Libris Systeme") sind in folgender Weise physisch gesichert:

1.1.1 Ex Libris Systeme befinden sich hinter verschlossenen Stahltüren und sind nur mit Kartenschlüsseln oder über biometrische Vorrichtungen zugänglich. Der Zugang ist nur autorisiertem Personal und nur in Begleitung möglich. Der Zugang zum Rechenzentrum wird rund um die Uhr überwacht.

1.1.2 Ex Libris Systeme sind nur mit Codeschlüsseln zugänglich und durch Alarmanlagen und/oder Videoüberwachungssysteme gesichert, wenn kein Personal vor Ort ist.

1.2 Ex Libris Systeme sind in folgender Weise vor Umwelteinflüssen geschützt:

1.2.1 Ex Libris Systeme befinden sich in einer Umgebung, deren Temperatur und Luftfeuchtigkeit kontrolliert wird; und

1.2.2 Ex Libris Systeme sind in einem Raum mit Feuerlöschanlage,

systems, CO2, or halon extinguishers.

1.3 Ex Libris Data Centers in Europe and Asia are ISO 27001 certified.

2 Network Security

2.1 Network and computer systems are protected by industry-standard firewalls and configured so that:

2.1.1 The firewall is configured to “Deny All” with inbound traffic explicitly authorized.

2.1.2 The firewall application and operating systems software updates are kept current.

2.1.3 Administrative access to the firewall and other perimeter devices is allowed only through secure methods (for example, SSL, VPN, SSH) or a direct serial port access.

2.1.4 Only authorized ports and protocols are allowed through the firewall.

2.2 An industry standard Intrusion Prevention System (IPS) is deployed within the environment and configured so that:

2.2.1 All signature and definition files are updated daily.

2.2.2 Known malicious network traffic is blocked.

2.2.3 Only authorized protocols and ports are allowed to traverse the network and firewall. All others are denied.

2.3 Network security events are analyzed, correlated, and evalu-

CO2- oder Halonanlage, untergebracht.

1.3 Ex Libris Rechenzentren in Europa und Asien sind ISO 27001 zertifiziert.

2 Netzwerksicherheit

2.1 Das Netzwerk und die Computersysteme sind durch branchenübliche Firewalls geschützt und wie folgt konfiguriert:

2.1.1 Die Firewall ist so eingestellt, dass sie nur explizit autorisierte einkommende Verbindungen zulässt.

2.1.2 Die Firewall und die verwendete Systemsoftware werden durch Updates auf dem neuesten Stand gehalten.

2.1.3 Der administrative Zugang zur Firewall und anderen Perimeter-Vorrichtungen ist nur bei Nutzung sicherer Methoden (z.B. SSL, VPN, SSH) oder eines direkten Zugangs über eine serielle Schnittstelle zulässig.

2.1.4 Nur autorisierte Ports und Protokolle werden von der Firewall zugelassen.

2.2 Ein dem Industriestandard entsprechendes System zur Abwehr von Angriffen (IPS) wird in der Umgebung eingesetzt und wie folgt eingestellt:

2.2.1 Alle Signatur- und Definitionsdateien werden täglich aktualisiert.

2.2.2 Als schädlich identifizierter Netzwerkverkehr wird blockiert.

2.2.3 Nur autorisierten Protokollen und Ports wird gestattet, die Firewall und das Netzwerk zu durchqueren. Allen anderen wird der Zugriff verwehrt.

2.3 Für die Netzwerksicherheit relevante Vorgänge werden rund

ated, 24x7 by Security Operations Center (“SOC”).

2.4 Ex Libris conducts at least annually external and internal penetration tests and vulnerability system scans to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems.

3 Operating System Management and Security

3.1 Third party operating systems used by Ex Libris Programs are the currently supported versions, for which such third party supplies security updates.

3.2 Operating System passwords for system access are managed according to ExLibris Password Management Policy which includes requirements for password expiration, strength and history/reuse.

3.3 Operating systems security events are analyzed, correlated, and evaluated, 24x7 by SOC

3.4 All security updates for the operating system layer (operating systems, device drivers, etc.) are kept current.

3.5 Procedures to remove system access are followed when an employee or contractor cease to be employed or to provide services.

3.6 Access to the operating system to perform remote administration is restricted to approved users and points of origin, and use secure tunnel or remote SSH with at least 256 bit encryption for both authentication and the session.

um die Uhr vom Security Operations Center („SOC“) zusammenhängend analysiert und ausgewertet.

2.4 Ex Libris führt mindestens jährlich externe und interne Penetrationstests und Schwachstellenanalysen durch, um mögliche Schwachstellen und Angriffsflächen zu identifizieren, die für einen Missbrauch der betrieblichen Systeme genutzt werden könnten.

3 Betriebssystemmanagement und -sicherheit

3.1 Bei von Dritten stammenden Betriebssystemen, die von Ex Libris Programmen genutzt werden, handelt es sich um vom Hersteller mit Sicherheitsupdates versorgte und aktuell unterstützte Versionen.

3.2 Systemzugangspasswörter von Betriebssystemen werden entsprechend der Ex-Libris Richtlinie für Passwortverwaltung verwaltet, die Regelungen zur Gültigkeitsdauer, zur Stärke und zur Historie/Wiederverwendung von Passwörtern vorgibt.

3.3 Für die Betriebssystemsicherheit relevante Vorgänge werden rund um die Uhr vom SOC zusammenhängend analysiert und ausgewertet.

3.4 Alle Sicherheitsupdates auf der Betriebssystemebene (Betriebssystem, Gerätetreiber usw.) werden auf dem neuesten Stand gehalten.

3.5 Endet die Tätigkeit eines Arbeitnehmers oder das Vertragsverhältnis mit einem Dienstleister, findet ein Verfahren zur Löschung seines Systemzugangs Anwendung.

3.6 Der Zugang zum Betriebssystem für Maßnahmen der Fernverwaltung ist begrenzt auf zugelassene Nutzer und Herkunftsorte, die sichere Tunnel- oder SSH-Remote-Verbindungen mit mind. 256-bit-Verschlüsselung sowohl für die Authentifizierung wie auch für die Session benutzen.

3.7 Change management procedures are in place and followed.	3.7 Change-Management-Verfahren werden eingesetzt und befolgt.
3.8 Products have security logging enabled that records successful and failed attempts of the following:	3.8 Die Produkte nehmen eine Sicherheitsprotokollierung der folgenden erfolgreichen oder gescheiterten Versuche vor:
3.8.1 Authentications;	3.8.1 Authentifizierungen;
3.8.2 User management actions (for example, user creation and password changes); and	3.8.2 Vorgänge der Nutzerverwaltung (z.B. Usererstellung und Passwortänderung); und
3.8.3 Access control changes (permissions changes to critical system and application components)	3.8.3 Zugangskontrolländerungen (Änderung von Freigaben, die kritische System- und Anwendungskomponenten betreffen)
3.9 Security event logs include at least the following information:	3.9 Sicherheitsvorfallprotokolle beinhalten mindestens folgende Informationen:
3.9.1 User identification;	3.9.1 Useridentifizierung;
3.9.2 Date and time of event;	3.9.2 Datum und Zeit des Vorgangs;
3.9.3 Indication of success or failure;	3.9.3 Angabe, ob erfolgreich oder nicht;
3.9.4 Origin of event; and	3.9.4 Herkunftsort des Vorgangs; und
3.9.5 Identity of affected resource	3.9.5 Identität der betroffenen Ressource
3.10 All security event logs are analyzed, correlated, and evaluated daily.	3.10 Alle Sicherheitsvorfallprotokolle werden täglich zusammenhängend analysiert und ausgewertet.
3.11 Antivirus software is deployed in the cloud environment.	3.11 Antivirussoftware wird in der Cloud-Umgebung eingesetzt.
3.12 The antivirus signatures are updated on a daily basis.	3.12 Die Antivirus-Signaturen werden täglich aktualisiert.
4 Application Security	**4 Anwendungssicherheit**
4.1 All security updates for the application layer (databases, application, etc.) are kept current.	4.1 Alle Sicherheitsupdates der Anwendungsebene (Datenbanken, Anwendungen usw.) werden auf dem neuesten Stand gehalten.
4.2 Procedures to remove application access are followed when an employee or contractor leaves the vendor’s organization or is ter-	4.2 Verfahren finden Anwendung, um sicherzustellen, dass der Anwendungszugang aufgehoben wird, wenn ein Arbeitnehmer oder

minated.

4.3 Change management procedures are in place and followed.

4.4 Products have security logging enabled that records successful and failed attempts of the following:

4.4.1 Authentications

4.4.2 User management actions (for example, user creation and password changes)

4.4.3 Access control changes (for example, permissions changes to critical system and application components)

4.5 Security event log connections at the OS level include at least the following information:

4.5.1 User identification

4.5.2 Date and time of event

4.5.3 Indication of success or failure

4.5.4 Origin of event

4.5.5 Identity of affected resource

4.6 All security event logs at the OS are analyzed, correlated, and evaluated daily.

5 Data Security

5.1 Data Protection

5.1.1 Ex Libris has internal policies and procedures in place with respect to unauthorized use, disclosure, loss, acquisition of or access to customer data.

Angestellter eines Dienstleisters die Organisation verlässt oder gekündigt wird.

4.3 Change-Management-Verfahren werden eingesetzt und befolgt.

4.4 Die Produkte nehmen eine Sicherheitsprotokollierung der folgenden erfolgreichen oder gescheiterten Versuche vor:

4.4.1 Authentifizierungen

4.4.2 Vorgänge der Nutzerverwaltung (z.B. Usererstellung und Passwortänderung)

4.4.3 Zugangskontrolländerungen (z.B. Änderung von Genehmigungen, die kritische System- und Anwendungskomponenten betreffen)

4.5 Sicherheitsvorgangsprotokolle auf dem OS-Level beinhalten mindestens folgende Informationen:

4.5.1 Useridentifizierung

4.5.2 Datum und Zeit des Vorgangs

4.5.3 Angabe, ob erfolgreich oder nicht;

4.5.4 Herkunftsort des Vorgangs

4.5.5 Identität der betroffenen Ressource

4.6 Alle Sicherheitsvorgangsprotokolle des OS werden täglich zusammenhängend analysiert und ausgewertet.

5 Datensicherheit

5.1 Datenschutz

5.1.1 Ex Libris hat interne Richtlinien und Verfahren zum Umgang mit der unautorisierten Nutzung, Offenlegung, dem Verlust sowie der unautorisierten Beschaffung von und Zugangsverschaffung zu Kun-

5.1.2 Customer data is stored, processed, and maintained solely on designated servers of Ex Libris (Deutschland) GmbH and no customer data at any time is transferred to any portable storage medium, unless that storage medium is in use as part of the designated backup and recovery processes.

5.2 Data Backup

5.2.1 Ex Libris is responsible for maintaining a backup of customer data, for an orderly and timely recovery of such data in the event that the service may be interrupted.

5.2.2 A documented and tested backup and recovery procedure must be in place.

5.2.3 Ex Libris stores a back of customer data in an off-site facility no less than weekly.

5.2.4 Ex Libris retains full backups for a period of no less than 4 weeks and incremental backups for a period of no less than 60 days.

5.3 Data Transmission

Ex Libris encrypts all Customer browser communications with the Program, using no less than 128 bit key length. This is accomplished using HTTPS, SFTP, or equivalent methods.

5.4 Data Sanitization

5.4.1 Storage medium containing customer data go through sanitization procedure before disposal or repurpose.

5.4.2 At a minimum, a “Clear” media sanitization is performed according to the standards enumerated by the National Institute of

dendaten.

5.1.2 Kundendaten werden ausschließlich auf bestimmten Servern der Ex Libris (Deutschland) GmbH gespeichert, verarbeitet und verwaltet und zu keiner Zeit auf tragbare Datenträger übertragen, es sei denn der Datenträger wird als Teil bestimmter Sicherungs- und Wiederherstellungsprozesse genutzt.

5.2 Datensicherung

5.2.1 Ex Libris ist verantwortlich für die Gewährleistung einer Sicherung der Kundendaten zum Zweck einer geordneten und zeitnahen Wiederherstellung solcher Daten im Falle einer Störung des Dienstes.

5.2.2 Ein dokumentiertes und getestetes Sicherungs- und Wiederherstellungsverfahren wird gewährleistet.

5.2.3 Ex Libris legt mind. wöchentlich eine Sicherungskopie der Kundendaten in einer Einrichtung außerhalb des Standorts an.

5.2.4 Ex Libris bewahrt vollständige Sicherungskopien für einen Zeitraum von mind. 4Wochen und inkrementelle Sicherungskopien für einen Zeitraum von mind. 60 Tagen auf.

5.3 Datenübermittlung

Ex Libris verschlüsselt alle Browserkommunikationen des Kunden mit dem Programm mithilfe einer Schlüssellänge von mind. 128-bit. Dies wird durch die Nutzung von HTTPS, SFTP oder entsprechenden Methoden erreicht.

5.4 Datenträgerbereinigung

5.4.1 Datenträger, die Kundendaten enthalten, durchlaufen einen Löschprozess vor ihrer Entsorgung oder Wiederverwendung für andere Zwecke.

5.4.2 Als Minimum erfolgt die vollständige Bereinigung eines Datenträgers nach den Standards, die vom National Institute of Standards in

Standards, Guidelines for Media Sanitization, SP800-88, Appendix A- see http://csrc.nist.gov/(Guidelines for Media Sanitization), SP800-88, in Anlage A genannt sind – vgl.Guidelines for Media Sanitization. Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-88, Gaithersburg. MD 20899-8930, September 2006.

5.4.3 The data sanitization method used follows the DoD 5220.22-M specifications (7-pass overwriting algorithm).

DoD 5220.22-M, February 28, 2006. NATIONAL INDUSTRIAL. SECURITY PROGRAM. OPERATING. MANUAL. February 2006.

6 Application Development

6.1 Ex Libris follows a documented Secure Software Development Lifecycle ("SDLC").

6.2 Ex Libris ensures that security reviews are included throughout the SDLC.

6.3 Ex Libris takes any actions necessary to protect information against reasonably anticipated threats to limit the likelihood that vulnerabilities in its products are exposed.

6.4 Ex Libris development team is trained in secure programming techniques that address common vulnerabilities as identified in the Open Web Application Security Project's (OWASP) "Top Ten Project" (or other generally recognized industry practices).

6.5 Ex Libris assigns explicit responsibility for overall security for the Programs during development, management, and operation of the Programs.

den Richtlinien zur Bereinigung von Datenmedien (Guidelines for Media Sanitization), SP800-88, in Anlage A genannt sind – vgl.Guidelines for Media Sanitization. Recommendations oft he National Institute of Standards and Technology, NIST Special Publication 800-88, Gaithersburg. MD 20899-8930, September 2006.

5.4.3 Das verwendete Verfahren zur Datenträgerbereinigung folgt den Spezifikationen in DoD 5220.22-M (7-pass overwriting algorithm).

DoD 5220.22-M, February 28, 2006. NATIONAL INDUSTRIAL. SECURITY PROGRAM. OPERATING. MANUAL. February 2006.

6 Anwendungsentwicklung

6.1 Ex Libris folgt einem Secure Software Development Lifecycle („SDLC")-Ansatz.

6.2 Ex Libris stellt sicher, dass Sicherheitsüberprüfungen im Rahmen des SDLC erfolgen.

6.3 Ex Libris nimmt alle notwendigen Schritte vor, um Informationen vor vorhersehbaren Bedrohungen zu schützen und so die Wahrscheinlichkeit zu senken, dass Schwachstellen in seinen Produkten bestehen.

6.4. Das Entwicklungsteam von Ex Libris ist im Umgang mit Techniken sicherer Programmierung geschult, mit deren Hilfe häufig vorkommende Schwachstellen, die z.B. im „Top Ten Project" vom Open Web Application Security Project (OWASP) identifiziert und vermieden werden können (Ex Libris wendet auch andere allgemein akzeptierte Industriestandards dazu an).

6.5 Ex Libris weist ausdrücklich die Verantwortlichkeiten für die Gesamtsicherheit der Programme während ihrer Entwicklung, ihrer Verwaltung und ihrem Betrieb zu.

6.6 Ex Libris has a well-documented procedure and framework for conducting code reviews.

6.7 Ex Libris utilizes Vulnerability Assessment Tool as part of the software development process to identify common programming errors. At a minimum this tool targets all common vulnerabilities identified in the current OWASP Top 10 application vulnerabilities.

7 Security Policies and Procedures

7.1 Ex Libris employs a Security Officer responsible for the development and implementation of security policies and procedures. The Security Officer has the appropriate combination of information security knowledge, skill, and experience to effectively carry out the assigned responsibilities.

7.2 The Security Officer is responsible for conducting a security risk assessment by independent 3rd party (at least annually) and chairs a quarterly security forum sharing security information and raising awareness of security vulnerabilities.

7.3 Ex Libris has an information security awareness program and information security policies covering all employees.

7.4 Policies and procedures that identify a security incident and require a response are in place.

7.5 Ex Libris notifies the customer when any system that stores customer data is subject to unauthorized access or in the event of a suspected data breach.

6.6 Ex Libris verfügt über gut dokumentierte Verfahren und Rahmenbedingungen zur Durchführung von Codeanalysen.

6.7 Ex Libris nutzt ein Werkzeug zur Schwachstellenanalyse als Teil des Softwareentwicklungsprozesses, um allgemeine Programmierfehler zu entdecken. Dieses Werkzeug entdeckt mind. alle in der aktuellen OWASP Top 10-Liste aufgeführten Schwachstellen.

7. Sicherheitsrichtlinien und –verfahren

7.1 Ex Libris beschäftigt einen Sicherheitsbeauftragten, der für die Entwicklung und Umsetzung von Sicherheitsrichtlinien und -verfahren verantwortlich ist. Der Sicherheitsbeauftragte hat ausreichende Kenntnisse in Informationssicherheit sowie die erforderlichen Fähigkeiten und Erfahrung, um die ihm übertragenen Aufgaben effizient zu erfüllen.

7.2 Der Sicherheitsbeauftragte ist verantwortlich für die Durchführung von Sicherheitsrisikoeinschätzungen durch einen unabhängigen Dritten (mind. jährlich) und veranstaltet einmal im Quartal ein Sicherheitsforum zur Weitergabe sicherheitsbezogener Informationen und zur Erhöhung des Bewusstseins für Sicherheitsschwachstellen.

7.3 Ex Libris verfügt über ein Programm zur Stärkung des Bewusstseins für Informationssicherheit und über Informationssicherheitsrichtlinien, an dem alle Angestellten teilnehmen.

7.4 Richtlinien und Verfahren, die Sicherheitsvorfälle erkennen und eine entsprechende Maßnahme anordnen, sind vorhanden.

7.5 Ex Libris informiert seine Kunden, wenn ein System, das Kundendaten speichert, einem unautorisierten Zugriff unterliegt oder ein vermuteter Datenschutzverstoß vorliegt.

7.6 Security Breach Notification

Ex Libris shall report to customer any use or disclosure of sensitive data not authorized by the customer. Ex Libris shall identify: (i) the nature of the unauthorized use or disclosure, (ii) the sensitive data used or disclosed, (iii) what corrective action Ex Libris has taken or shall take to prevent future similar unauthorized use or disclosure.

7.7 Before the implementation process may start, the Controllers will jointly conduct a risk analysis and draft a security concept according to the requirements of the Berlin Data Protection Act. Ex Libris will support the Universities during this process. If risks are identified during this process that, in view of the requirements of the Berlin Data Protection Act, make adjustments to the above necessary, then the parties will agree on how to implement the adjustments.

7.8 The data protection officers of the universities should before operation perform a data protection review of the system in coordination with the BBDI. This procedure must be taken into account in the development and submission of the security concept by granting a reasonable advance period. The Controller is entitled to refuse consent to the "go live" for as long as defects brought to light by the test result of the data protection officers of the universities in coordination with the BBDI are deemed not to have been adequately resolved. The parties undertake, in consideration of permissible changes in accordance with Art. 3, para. 3 Annex 7a, to comply with the SiKo agreed in this way.

7.6 Meldepflicht bei Sicherheitsverstößen

Ex Libris wird seine Kunden über jede von diesem nicht autorisierte Nutzung oder Offenlegung sensibler Daten informieren. Dabei wird Ex Libris mitteilen (i) welcher Art die unautorisierte Nutzung oder Offenlegung war, (ii) welche sensiblen Daten genutzt oder offen gelegt wurden, (iii) welche Maßnahmen Ex Libris getroffen hat oder treffen wird, um eine ähnliche unautorisierte Nutzung oder Offenlegung in der Zukunft zu verhindern.

7.7 Bevor die Implementierung beginnen kann, werden die Auftraggeberinnen gemeinsam eine Risikoanalyse durchführen und ein Sicherheitskonzept entwerfen. Ex Libris wird die Universitäten in diesem Prozess unterstützen. Sollten Risiken identifiziert werden, die, entsprechend der Anforderungen des Berliner Datenschutzgesetzes, Anpassungen der vorstehenden Maßnahmen notwendig machen, werden sich die Parteien einigen, wie diese umgesetzt werden können.

7.8 Die behördlichen Datenschutzbeauftragten der Hochschulen nehmen vor Inbetriebnahme eine datenschutzrechtliche Bewertung des Systems in Abstimmung mit dem BBDI vor. Diesem Ablauf ist bei der Entwicklung und Einreichung des Sicherheitskonzepts durch Einräumung eines angemessenen zeitlichen Vorlaufs Rechnung zu tragen. Die Auftraggeberin ist berechtigt, die Zustimmung zum „Go live“ zu verweigern, solange nach dem Prüfergebnis der behördlichen Datenschutzbeauftragten der Hochschulen in Abstimmung mit dem BBDI geltend gemachte Mängel als nicht angemessen ausgeräumt zu erachten sind. Die Parteien verpflichten sich, unter Berücksichtigung zulässiger Änderungen gem. § 3 Abs. 3 Anhang 7a, das so abgestimmte SiKO einzuhalten.