Technische und organisatorische Maßnahmen nach Art. 32 DSGVO für die HPI Schul-Cloud International

Stand: 03.03.21

Nachfolgend werden die technischen und organisatorischen Maßnahmen zur Gewährleistung eines angemessene Datenschutz- und Datensicherheitsniveau in der HPI Schul-Cloud International beschrieben. Die Maßnahmen begegnen insbesondere den cloud-spezifischen Sicherheitsrisiken, die dadurch entstehen, dass die Cloudnutzer keinen unmittelbaren Zugriff auf die Cloudinfrastruktur haben (vgl. dazu Orientierungshilfe Cloud Computing der Datenschutzkonferenz und Düsseldorfer Kreises, Version 2.0, S. 27 ff.) und berücksichtigen die besondere Sensibilität der verarbeiteten Daten der Schüler*innen, Eltern und Lehrenden.

1. Maßnahme zur Pseudonymisierung

Maßnahmen, die den unmittelbaren Personenbezug während der Verarbeitung in einer Weise reduzieren, dass nur mit Hinzuziehung zusätzlicher Informationen eine Zuordnung zu einer spezifischen betroffenen Person möglich ist. Die Zusatzinformationen sind dabei durch geeignete technische und organisatorische Maßnahmen von dem Pseudonym getrennt aufzubewahren.

Unpseudonymisierte Daten der HPI Schul-Cloud International dürfen nicht für Außenstehende sichtbar sein. Jede/r Schüler*in verfügt in der HPI Schul-Cloud International über eine eindeutige Identifikationsnummer, mit der sich alle gespeicherten Eigenschaften der Schüler*innen (z.B. E-Mail-Adresse, Telefonnummer, Schule, Klasse, IP-Adresse) aus einer entsprechenden Datenbank zuordnen lassen.

Schüler*innen haben bei jedem externen Inhalte-Anbieter ein Pseudonym (UUID), sodass Lernfortschritte zwar gespeichert werden können, der Inhalteanbieter jedoch keine Information über die wahre Identität bzw. gespeicherten Daten der dahinterstehenden Person erhalten. Feedback-Daten (getätigte Vorgänge, z.B. Schüler Pseudo XYZ hat das Thema lineare Gleichungen in bettermarks absolviert oder Schüler Pseudo XYZ hat Lernvideo in bettermarks abgespielt) von Inhalteanbietern werden mithilfe der xAPI bzw. einer clientseitigen Bibliothek übertragen. Die Durchführung der Pseudonymisierungsverfahren erfolgt automatisch. Auch die eingehenden geheimen Parameter der Pseudonymisierung werden automatisch und zufällig erzeugt. Die Depseudonymisierung der Nutzerdaten erfolgt automatisch an berechtigte Lehrkräfte, also nur für die in diesem Kurs eingeschriebenen Schüler*innen mit den zu diesem Kurs gehörigen Nutzerdaten. Ausschließlich HPI Schul-Cloud International-Administratoren haben Zugriff auf die Zuordnungstabellen.

2. Maßnahmen zur Verschlüsselung

Maßnahmen oder Vorgänge, durch die eine klar lesbare Information mit Hilfe eines Verschlüsselungsverfahrens in eine nicht ohne Weiteres interpretierbare Zeichenfolge (Geheimtext) umgewandelt wird.

Der Zugriff auf die HPI Schul-Cloud International ist für die Nutzer von außen ausschließlich über HTTPS möglich, sodass eine Transportverschlüsselung der Anfragen und Antworten erfolgt (Verschlüsselungszertifikat nach dem jeweiligen Stand der Technik, derzeit TLS 1.2).

Mitarbeiter der HPI Schul-Cloud International greifen von außen auf interne Infrastruktur und Daten über eine verschlüsselte Netzwerkverbindung über das SSH-Protokoll zu. Wie die Infrastruktur sind auch Backups innerhalb dieses Netzwerks nur

über verschlüsselte Verbindungen (SSH und VPN) verfügbar und werden innerhalb dessen sicher erstellt und transferiert.

3. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend der Weisungen des Auftraggebers verarbeitet werden können.

Die HPI Schul-Cloud International stellt eine Software as a Service (SaaS)-Lösung für Schulen dar, damit diese moderne digitale Lehr- und Lerninhalte online nutzen können. Die HPI Schul-Cloud International wird daher auf den Servern von ausgewählten Hosting-Anbietern gehostet, um jederzeit eine zuverlässige, sichere und schnelle Verfügbarkeit aller Daten und Inhalte auf den unterstützen Endgeräten zu gewährleisten. Neben dem Front- und Backend der HPI Schul-Cloud International werden auf diesen Servern auch sämtliche in der HPI Schul-Cloud International verarbeitete Daten sowie Backups gespeichert. Erfasst sind insbesondere auch die im Auftragsverarbeitungsvertrag benannten personenbezogenen Daten.

Daneben arbeitet das HPI auch mit ausgewählten Inhalte-Anbietern zusammen, deren akademische Inhalte im Lern-Store der HPI Schul-Cloud International verlinkt werden. Grundsätzlich erhalten die Inhalte-Anbieter keine personenbezogenen Daten vom HPI. Sofern die Inhalte-Anbieter im Rahmen von ihnen angebotenen Inhalte und Webanwendungen personenbezogene Daten verarbeiten sollten, so findet diese Verarbeitung grundsätzlich in eigenständiger datenschutzrechtlicher Verantwortlichkeit der Inhalte-Anbieter statt. Jedoch erhalten ausgewählte Inhalte-Anbieter beim Aufruf ihrer Inhalte ein vom HPI erstelltes, nutzerspezifisches Pseudonym, da nur so die Lernfortschritte der Nutzer in festgehalten werden können. In diesem Fall schließt das HPI vorher mit den betroffenen Inhalte-Anbietern einen Auftragsverarbeitungsvertrag nach Art. 28 DSGVO, durch die weisungs- und zweckgebundene Verarbeitung der Pseudonyme sichergestellt wird. Ausschließlich Administratoren*innen der HPI Schul-Cloud International haben Zugriff auf die Zuordnungstabellen für die Pseudonyme. Das HPI übermittelt darüber hinaus keine personenbezogenen Daten an die Inhalte-Anbieter.

3.1 Auswahl von Dienstleistern

Zu den im Rahmen der HPI Schul-Cloud International zum Einsatz kommenden Dienstleistern zählen, die zuvor erwähnten Hosting- und Inhalte-Anbieter, sofern diese personenbezogene Daten vom HPI erhalten. Die eingesetzten Dienstleister werden ausschließlich auf Basis eines schriftlichen Vertrags in Übereinstimmung mit den Bestimmungen über Unterauftragsverhältnisse gemäß dem Auftragsverarbeitungsvertrag mit den Schulen in Anspruch genommen. Die Auswahl der Unterauftragnehmer erfolgt entsprechend Art. 28 Abs. 1 DSGVO insbesondere in Hinsicht auf die Datensicherheit mit besonderer Sorgfalt. Die Dienstleister werden vom HPI vertraglich zur Einhaltung eines Datenschutzniveaus verpflichtet, das dem im Auftragsverarbeitungsvertrag mit den Schulen entspricht.

Das HPI informiert die Schulen über alle eingesetzten Dienstleister und beabsichtigte Änderungen. Nach Beendigung des Auftrags wird die datenschutzkonforme Löschung der auftragsgegenständlichen Daten durch die Dienstleister veranlasst. Eine aktuelle Liste der aller derzeit eingesetzten Dienstleister kann online im *Verzeichnis aller Empfänger personenbezogener Daten*[1] eingesehen werden.

[1] https://s3.hidrive.strato.com/schul-cloud-hpi/int/Dokumente/Empfaenger.pdf

3.2 Auftragskontrolle der Inhalte-Anbieter

Sofern einzelne Inhalte-Anbieter, wie unter Ziffer 3.1 – *Auswahl von Dienstleistern* beschrieben, pseudonymisierte Daten der Nutzer erhalten, verpflichten sich diese Inhalte-Anbieter im Auftragsverarbeitungsvertrag mit dem HPI, keine weiteren Auftragsverarbeiter ohne die vorherige gesonderte Genehmigung des HPI in Anspruch zu nehmen. Bei Einschaltung von Unterauftragnehmern durch die Inhalte-Anbieter muss stets ein Schutzniveau, das mit demjenigen des Auftragsverarbeitungsvertrag mit dem HPI vergleichbar ist, gewährleistet werden.

3.3 Auftragskontrolle der Hosting-Anbieter

Mit dem Hosting ist die dataport AöR, Altenholzer Straße 10-14, 24161 Altenholz beauftragt. Sie verpflichtet die von ihr beauftragten Unterauftragnehmer im gesetzlich erforderlichen Umfang nach Art. 28 DSGVO. Die von den Hosting-Dienstleistern eingesetzte Unterauftragnehmer sind:

- 1&1 IONOS SE, Elgendorfer Str. 57, 56410 Montabaur, Deutschland (als weiterer Auftragsverarbeiter von dataport AöR)
- Cronon GmbH, Pascalstraße 10, 10587 Berlin, Deutschland (als weiterer Auftragsverarbeiter von 1&1 IONOS SE)

Darüber hinaus werden vom HPI aktuell die folgenden Anbieter Beispielsweise für die Ablage von hochgeladenen Nutzerdaten, Backups oder für den Lern-Store beauftragt:

- STRATO AG, Pascalstraße 10, 10587 Berlin
- Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen

3.4 Standort und Sicherheitskonzept der Hosting-Anbieter

Das HPI nutzt ausschließlich Hosting-Anbieter mit Geschäftssitz und Serverstandorten in Deutschland. Die genutzten Rechenzentren der Hosting-Anbieter befinden sich in verschiedenen deutschen Städten und kommen abhängig vom jeweiligen Standort des Nutzers und der aktuellen Auslastung der Infrastruktur zum Einsatz. Alle verwendeten Rechenzentren sind nach ISO/IEC 27001 zertifiziert und Kopien der aktuellen Zertifikate liegen vor, womit ein wirksames Informationssicherheits-Managementsystem nachgewiesen wird.

Das HPI arbeitet derzeit mit folgenden Hosting-Dienstleistern zusammen:

Name/ Anschrift	**Ort der Verarbeitung**	**ISO/IEC-Zertifizierung**	**Informationen zur Datensicherheit**
1&1 IONOS SE, Elgendorfer Str. 57, 56410 Montabaur (als weiterer Auftragsverarbeiter von dataport AöR)	Deutschland	ISO/IEC 27001:2013	IONOS-TOM[2]

[2] https://www.ionos.de/terms-gtc/fileadmin/pdf/terms-gtc/DE/Enterprise_Cloud/2020/Anlage_4_Technisch-organisatorische_Massnahmen.pdf

Cronon GmbH, Pascalstraße 10, 10587 Berlin, Deutschland (als weiterer Auftragsverarbeiter von 1&1 IONOS SE)	Deutschland	ISO/IEC 27001	
Hetzner Online GmbH Industriestr. 25 91710 Gunzenhausen	Deutschland	ISO/IEC 27001:2013	Hetzner-TOM[3]
STRATO AG Pascalstr. 10 10587 Berlin	Deutschland	ISO/IEC 27001:2013	SRATO-Sicherheitskonzept[4]

3.5 Aufgabenspezifische technische und organisatorische Maßnahmen

Im Rahmen der HPI-Schul Cloud kann grob zwischen zwei Aufgabensphären unterschieden werden: (1) Das HPI greift zu den vertraglich vorgesehen Zwecken, insbesondere Aktualisierung, Pflege und Wartung der HPI Schul-Cloud International auf die Server der Hosting-Anbieter zu. Der Fernzugriff durch die Mitarbeiter*innen des HPI erfolgt über vom HPI autorisierte Endgeräte. (2) Die Verarbeitung durch die Hosting-Anbieter beschränkt sich hingegen auf die Bereitstellung der Hardware, das Hosting und die IT-Wartung. Soweit die getroffenen technischen und organisatorischen Maßnahmen zwischen diesen beiden Aufgabensphären differenzieren, werden nachfolgend die Maßnahmen als solche der HPI bzw. der Hosting-Dienstleister ausgewiesen.

Es werden nur solche Maßnahmen berücksichtigt, die von allen Hosting-Anbietern gleichermaßen getroffen werden. Dadurch ist sichergestellt, dass die Maßnahmen unabhängig davon greifen, von welchem konkreten Anbieter die Daten verarbeitet werden.

4. Gewährleistung der Vertraulichkeit

4.1 Zutrittskontrolle

Maßnahmen, die unbefugten Personen den Zutritt zu Datenverarbeitungsanlagen verwehren.

a. Maßnahmen des HPI

Das Institut ist über ein elektronisches Zugangssystem mit Türsicherung gesichert, sodass Unbefugte die Räumlichkeiten nicht betreten können. Es gibt keine ungesicherten Zugänge zum Institut. Die Hauptzugänge des Instituts sind zusätzlich mit Kamera und Bewegungsmeldern gesichert. Besucher*innen müssen von einem / einer Mitarbeiter*in empfangen werden, andernfalls wird der Zutritt zum Gebäude durch den Empfang verwehrt, sodass stets eine Personenkontrolle stattfindet. Es existiert sowohl eine Transponder- als auch eine Schließordnung, die Ausgabe von Transpondern wird stets protokolliert. Außerhalb der allgemeinen Öffnungszeiten ist

[3] https://www.hetzner.com/AV/TOM.pdf

[4] https://www.strato.de/sicherheit/

das Institut über eine Alarmanlage gesichert. Das Wachpersonal ist sorgfältig ausgewählt.

b. Maßnahmen der Hosting-Anbieter

Die vom HPI ausgewählten Hosting-Anbieter gewährleisten einen wirksamen Zutrittsschutz für alle verwendeten Datenverarbeitungsanlagen. Dabei wird jeder Zutritt zu den Räumlichkeiten mit Datenverarbeitungsanalgen elektronisch kontrolliert und protokolliert. Zudem verwalten und überprüfen die Hosting-Anbieter den Kreis der Personen, denen Zutritt zu den Räumlichkeiten gewährt wird. Fremdpersonal und sonstige betriebsfremde Personen werden stets von zutrittsberechtigtem Personal der Hosting-Anbieter begleitet. Schließlich werden die Räumlichkeiten durch Sicherheitspersonal, Kameras oder vergleichbare Maßnahmen überwacht.

4.2 Zugangskontrolle

Maßnahmen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

a. Maßnahmen des HPI

Die Authentifikation ins Datenverarbeitungssystem der HPI Schul-Cloud International erfolgt mit Benutzernamen und Passwort. Verschiedene Benutzerrechte sind je nach Berechtigung vergeben. Benutzerprofile, die beim Eintritt ins Institut angelegt und bei Austritt umgehend gelöscht werden, sind dem IT-System zugeordnet, sodass stets eine eindeutige Identifikation erfolgt. Benutzer*innen erhalten dadurch nur Zugang zu den Netzdiensten, zu deren Nutzung sie ausdrücklich befugt sind. Auch das WLAN ist so vor unbefugtem Zugang gesichert. Passwörter müssen nach gängigen BSI-Sicherheitsstandards mit vorgegebener minimaler Passwortlänge erstellt sowie regelmäßig (mindestens halbjährlich) neu vergeben werden.

Das Datenverarbeitungssystem der HPI Schul-Cloud International wird sowohl mittels Software-Firewall als auch Anti-Viren-Software geschützt. Der Netzzugang wird mittels VPN-Technologie ermöglicht. Die Zugangsberechtigungen werden regelmäßig (mindestens alle 3 Monate, in der Regel umgehend bei Ein- und Austritt) auf Gültigkeit überprüft. Mobile Datenträger werden verschlüsselt. Dies betrifft insbesondere auch die Backup-Systeme. Die Verwaltungs-Systeme des HPI verfügt darüber hinaus über ein Intrusion Detection System.

Der Zugang zu den Datenverarbeitungssystemen des HPI ist mit Sicherheitsschlössern und einer Schlüsselregelung gesichert, sodass ein unbefugter Zugang auf dieser Ebene ausgeschlossen ist. Datenträger oder Geräte können bei Wartungsarbeiten die Räumlichkeiten nicht unkontrolliert verlassen, da ein Zugang nur durch Anweisung und unter Aufsicht erfolgt.

Die technischen Maßnahmen werden durch zahlreiche organisatorische Maßnahmen des HPI, insbesondere Richtlinien zum Umgang mit den Daten, begleitet.

b. Maßnahmen der Hosting-Anbieter

Der Zugang zu den Administrationsbereichen der Server ist durch sichere Zugangsverfahren geschützt. Es müssen Passwörter mit angemessener Passwortlänge verwendet werden.

Zudem ermöglichen die Hosting-Anbieter es dem HPI, das Zugriffs- und Berechtigungskonzept des HPI in der Serverumgebung der Anbieter umzusetzen und Serverzugriffe zu protokollieren. Darüber hinaus erfolgt teilweise auch zusätzlich eine systemseitige Protokollierung der Zugänge durch die Hosting-Anbieter.

4.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass Daten bei der Verarbeitung, Nutzung und Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

a. Maßnahmen des HPI

Die Zugriffe werden durch das HPI kontrolliert. Eine Übersicht, in welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können, wurde erstellt. Ein Berechtigungskonzept zur Zugriffskontrolle dieser Daten wurde ebenso erstellt. Die Vergabe von Rechten zur Eingabe, Änderung und Löschung von erhobenen Daten erfolgt auf Basis dieses Berechtigungskonzepts. Berechtigungen für normale Nutzer (Schüler*innen, Lehrende) und Administrator*innen (Schuladministrator*innen, HPI Schul-Cloud International-Systemadministrator*innen) sind getrennt. Die Rechte werden durch die HPI Schul-Cloud International-Systemadministrator*innen verwaltet. Die vergebenen Berechtigungen werden regelmäßig von den HPI Schul-Cloud International-Administrator*innen kontrolliert. Die Zahl der Nutzer*innen mit administrativen Rechten ist auf ein notwendiges Minimum reduziert.

Die Protokollierung der Eingabe, Änderung und Löschung von Daten ist integriert. Diese werden manuell und stichprobenartig kontrolliert.

Formulare, die personenbezogene Daten enthalten, werden ausschließlich digital erstellt und entgegengenommen, sodass keine physikalischen Dateien aufbewahrt werden müssen.

b. Maßnahmen der Hosting-Anbieter

Seitens der Hosting-Anbieter werden Daten durch Verschlüsselung vor unberechtigten Zugriffen geschützt. Anwendungs- und Administrationszugänge werden getrennt. Zugriffsversuche werden elektronisch protokolliert.

4.4 Mandantentrennung

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden und so von anderen Daten und Systemen getrennt sind, sodass eine ungeplante Verwendung dieser Daten zu anderen Zwecken verhindert wird.

Die Trennung der Mandanten wird durch das HPI gewährleistet. Verschiedene Anwendungsfälle verfügen über verschiedene, eigenständige IT-Systeme. Datenbankrechte wurden spezifiziert. Eine Trennung von Zuordnungsdateien sowie der Aufbewahrung auf einem getrennten, abgesicherten IT-System erfolgt bei pseudonymisierten Daten.

Produktiv- und Testsystem sind voneinander getrennt, um einen unterbrechungs- und fehlerfreien Betrieb sowie die Datensicherheit stets zu gewährleisten. Die Entwicklung erfolgt stets mit manuell erzeugten Testdaten, sodass hier kein unautorisierter Zugriff auf tatsächliche Daten oder das Ändern von Produktivdaten möglich ist. Testdaten, die auf Echtdaten basieren, werden anonymisiert. Die verschiedenen Instanzen der HPI Schul-Cloud (BMBF-Projekt, Niedersächsische Bildungscloud, Schul-Cloud Brandenburg, Thüringer Schul-Cloud, HPI Schul-Cloud International) liegen jeweils auf eigenen Servern und somit getrennten Datenbanken. Instanzenübergreifend kann kein Zugriff erfolgen. Innerhalb einer Instanz greifen

allen Schulen auf dieselbe Datenbank zu, haben jedoch keinen direkten Zugriff auf die Datenbank über die API.

4.5 Weitere Maßnahmen zur Gewährleistung der Vertraulichkeit

Administratoren-Accounts werden automatisch nach 30 Minuten Inaktivität aus der HPI Schul-Cloud International ausgeloggt. Die übrigen Nutzer-Accounts werden nach 120 Minuten Inaktivität automatisch ausgeloggt. Wenige Minuten vor dem Log-out erscheint ein Fenster, das auf den bevorstehenden automatischen Log-out hinweist. Der Nutzer kann jedoch beim Log-in auch die Option auswählen, dass er auf dem verwendeten Endgerät eingeloggt bleiben möchte. In diesem Fall erfolgt der automatische Log-out erst nach 30 Tagen.

Um auch die Gewährleistung der Vertraulichkeit beim Einsatz der HPI Schul-Cloud International in den Schulen und zu Hause sicherzustellen, wurden verschiedene Checklisten für Lehrende und Schüler*innen sowie Schuladministrator*innen erstellt. Diese beschreiben relevante Maßnahmen für

- Schüler*innen, z.B. zu den Themen Privatsphäre, Zugangsdaten, oder Passwortsicherheit und
- Lehrende zusätzlich zu den Maßnahmen für Schüler*innen z.B. mit Hinweisen zur Nutzung von Privatgeräten und Hotspots sowie dem Verbot des Speicherns sensibler Daten bzw. dem Hinweis, welche Daten mit der HPI Schul-Cloud International verarbeitet werden dürfen.

5. Gewährleistung der Integrität

5.1 Weitergabekontrolle

Maßnahmen die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

a. Maßnahmen des HPI

Mitarbeiter*innen sind dazu verpflichtet, einen ausreichenden Schutz der Geräte sicherzustellen (Sperren des Bildschirms, Verschließen des Raumes), wenn diese unbeaufsichtigt sind, sowie Unterlagen mit relevanten Daten (insbesondere personenbezogen) nicht unnötig lange auf Schreibtischen aufzubewahren, sondern diese sicher zu verwahren bzw. vernichten. Öffentlich verfügbare APIs werden neben dem JWT-Token zusätzlich über ein Shared-Key-Verfahren gesichert. Die sichere Übertragung personenbezogener Daten wird durch VPN-Tunnel gewährleistet. Gängige Sicherheitsprotokolle werden verwendet.

In Bezug auf die Transportverschlüsselung beim Zugriff auf die HPI Schul-Cloud International wird auf Ziffer 2 – *Maßnahmen zur Verschlüsselung* verwiesen.

b. Maßnahmen der Hosting-Anbieter

Mitarbeiter*innen der Hosting-Anbieter sind zur Vertraulichkeit im Umgang mit personenbezogenen Daten verpflichtet. Daten werden mit Verschlüsselungsverfahren (TLS 1.2+) übertragen, die dem Stand der Technik entsprechen. Die auftragsgegenständlichen Daten werden datenschutzkonform gelöscht.

5.2 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind.

Die Eingabekontrolle wird vom HPI durchgeführt. Das HPI protokolliert die Systemaktivitäten der HPI-Schul-Cloud. Die Protokollierung der Logins ist integriert. Die Protokolle werden nach 14 Tagen gelöscht. Es existiert ein Berechtigungskonzept, vgl. dazu auch 4.3.

6. Gewährleistung der Verfügbarkeit

6.1 Maßnahmen des HPI

Das Datenverarbeitungssystem der HPI Schul-Cloud International wird sowohl mittels Software-Firewall als auch Anti-Viren-Software geschützt. Eingesetzte Systeme und Software werden regelmäßig gewartet und aktualisiert. Insbesondere bei Bekanntwerden von kritischen Sicherheitslücken wird die Software-Aktualisierung umgehend vorgenommen. Bei Sicherheitslücken von in der HPI Schul-Cloud International eingesetzter Fremdsoftware kommt das von GitHub gebotene Feature zur Warnung von Software-Updates mit sicherheitskritischen Aktualisierungen zum Einsatz.

Das HPI verfügt über einen Notfallplan sowie ein Backup & Recovery-Konzept. Es werden regelmäßige verschlüsselte Backups (auf separaten Backup-Servern im 6-stündigen Rhythmus) erstellt.

Autorisierte Zugriffe von außerhalb des Instituts werden mithilfe einer VPN-Verbindung gesichert (siehe Ziffer 6 – *Zugriffskontrolle*). Insofern Dokumente versandt bzw. extern zugreifbar abgelegt werden (hier werden ausschließlich Dokumentationen, aber keine personenbezogenen Daten verschickt), wird der Zugriff bei Bedarf mit einem Passwort gesichert.

Neue Entwicklungen in Form von Features und Hotfixes werden über einen Release- und Patchmanagementprozess verwaltet und eingespielt. Die Entwicklungen werden vor dem Einspielen sowohl automatisch als auch händisch getestet.

6.2 Maßnahmen der Hosting-Anbieter

Die von den Hosting-Anbietern eingesetzte Hardware ermöglicht eine redundante und damit unterbrechungsfreie Stromversorgung. Zudem treffen die Hosting-Anbieter Maßnahmen, um systembelastenden Missbrauch der Server, wie DDoS-Attacken, abzuwehren. Schließlich findet ein systematisches Monitoring der Server statt.

7. Gewährleistung der Belastbarkeit und raschen Wiederherstellbarkeit

7.1 Maßnahmen des HPI

Die Gewährleistung der Belastbarkeit (z.B. bei Angriffen) von Systemen wird durch jährliche Stresstests sichergestellt. Bei Bekanntwerden von Schwachstellen der Belastbarkeit werden umgehend technisch angemessene Maßnahmen ergriffen.

In Ziffer 6 – *Gewährleistung der Verfügbarkeit* wurden Maßnahmen beschrieben, die dem Abwenden, Erkennen und Bewältigen physischer oder technischer Zwischenfälle dienen, sowie die Wiederherstellbarkeit und die Funktionsfähigkeit dieser gewährleisten. Durch automatisches Monitoring der Produktivsysteme mit E-Mail-Benachrichtigung werden außerdem Zwischenfälle mit den Servern schnell (in der Regel innerhalb eines Arbeitstages) erkannt, sodass unverzügliches Handeln möglich ist. Insofern notwendig, werden nach einem Zwischenfall die Backup-Daten in das System eingespielt oder Sicherheitsmaßnahmen erhöht.

7.2 Maßnahmen der Hosting-Anbieter

Alle Hosting-Anbieter verfolgen einen Notfallplan, um die rasche Wiederherstellbarkeit aller für die Datenverarbeitung relevanten Systeme bei physischen oder technischen Zwischenfällen rasch wiederherzustellen.

Die Hosting-Anbieter haben ein Informationssicherheitsmanagementsystem eingerichtet, das nach ISO/IEC 27001 zertifiziert ist. Danach müssen die Anbieter wirksame Prozesse zur Reaktion auf Informationssicherheitsvorfälle und Wiederherstellungsmaßnahmen im Fall des Angriffs durch Schadsoftware bereithalten. Es werden Wiederherstellungstests durchgeführt.

8. Überprüfung, Bewertung und Evaluierung

8.1 Datenschutz-Management

a. Maßnahmen des HPI

Die HPI Schul-Cloud International verfolgt die Privacy-by-Design-Maxime, es werden also datenschutzfreundliche Voreinstellungen vorgenommen.

Ein Datenschutzbeauftragter ist für das Institut bestellt, für den keine Interessenkonflikte bestehen. Die Kontaktdaten des oder der Datenschutzbeauftragten sind veröffentlicht. Die Geschäftsführung unterstützt den Datenschutzbeauftragten. Der Datenschutzbeauftragte ist der Geschäftsführung direkt unterstellt und berichtet direkt an diese. Der Datenschutzbeauftragte verfügt über die für die Erfüllung seiner Aufgaben erforderlichen Mittel. Er wird bei der Planung neuer Verfahren oder der Änderung bestehender Verfahren rechtzeitig informiert und einbezogen, und gestaltet diese aktiv mit. Neue Mitarbeiter*innen erhalten Informationen zum Datenschutz bei dem Umgang mit personenbezogenen Daten. Personen, die personenbezogene Daten erheben, verarbeiten oder nutzen, sind durch Datenschutzschulungen auf datenschutzgerechtes Verhalten am Arbeitsplatz unterrichtet. Der Datenschutzbeauftragte kontrolliert stichprobenartig die Einhaltung der Richtlinien. Es wurde außerdem ein Informationssicherheitsbeauftragter für das Unternehmen bestellt.

Die Dokumente zu IT-Sicherheit und Datenschutz werden jährlich überarbeitet. In diesem Zusammenhang wird auch die Wirksamkeit der Maßnahmen bewertet. Bei Bekanntwerden eines entsprechenden Bedarfs bzw. neu auftretenden Schwachstellen werden die Maßnahmen aktualisiert. Es wird jährlich ein Prüfbericht erstellt.

Eine Datenschutz-Folgenabschätzung wird bei Bedarf durchgeführt.

Es bestehen formalisierte Prozesse für die Bearbeitung von Auskunftsanfragen seitens Betroffener sowie Datenschutzvorfällen.

Schließlich bereitet das HPI derzeit eine eigene Sicherheitszertifizierung nach ISO/IEC 27001 vor.

b. Maßnahmen der Hosting-Anbieter

Die Hosting-Anbieter verfügen über Informationssicherheitsmanagementsystem, das nach ISO/IEC 27001 zertifiziert ist. Zudem werden die technischen und organisatorischen Maßnahmen nach einem vorgegebenen Prozess regelmäßig überprüft.