Freie Universität Berlin

Freie Universität Berlin

Zugriff auf schützenswerte Daten der Freien Universität Berlin durch Externe

Handlungsleitfaden

Fassung: Juni 2009

Inhalt

1 Einleitung 3

2 Aspekte des Zugriffs auf schützenswerte Daten 4

3 Workflow 6

3.1 Neues Projekt bzw. Vorhaben 6

3.1.1 Phase 1 – Beteiligung prüfen 8

3.1.2 Phase 2 – Erstellung der Leistungsbeschreibung / Verdingungsunterlagen 8

3.1.3 Phase 3 – Prüfung der Unterlagen auf Einhaltung der Sicherheits- und Datenschutzstandards 8

3.1.4 Phase 4 – Prüfung durch die Auftrag vergebende Stelle (Vergabestelle) 8

3.1.5 Phase 5 – Fertigstellung der vertragsrelevanten Unterlagen 9

3.1.6 Phase 6 – Zuschlagserteilung bzw. Vertragsabschluss 9

3.2 Bestehendes Projekt bzw. IT-Verfahren 9

4 Checkliste 10

5 Anlage: Mustervereinbarung für Auftragsdatenverarbeitung 12

6 Verzeichnis der zitierten Gesetze 16

Autoren: Arbeitsgruppe „Datenzugriff“

Herr J. Bechlars (ZEDAT)
Frau G. Buchholz (eAS)
Herr D. Dräger (eAS)
Herr Dr. A. Geukes (CeDiS)
Herr G. Haese (CeDiS)
Herr J. Kende (UB)
Frau H. Kilanski (GPR)
Frau A. Kiwitt (eAS)
Frau S. Krebs-Pahlke (PRD)
Frau A. Müller (UB)
Frau I. Pahlen-Brandt (DS)
Frau A. Syring (eAS)

1 Einleitung

Der vorliegende Handlungsleitfaden regelt verbindlich die Vorkehrungen und Maßnahmen zur Kontrolle von Zugriffen auf schützenswerte Daten der Freien Universität Berlin durch externe Personen. Gemäß der Definition in der IT-Sicherheitsrichtlinie der Freien Universität Berlin werden unter „schützenswerte Daten“ Informationen verstanden, deren Verlust, Bekanntwerden oder Verfälschung einen erheblichen materiellen und immateriellen Schaden bedeutet. Demgemäß kann es sich bei schützenswerten Daten zum Beispiel um personenbezogene Daten der Beschäftigten oder um Messergebnisse im Rahmen von Forschungsarbeiten handeln. Der Schutzbedarf muss mit Hilfe der in der IT-Sicherheitsrichtlinie beschriebenen Schutzbedarfsanalyse ermittelt werden. In diesem Leitfaden sind „externe Personen“ Personen, die in keinem Beschäftigungsverhältnis zur Freien Universität Berlin stehen und auch sonst zu keiner der Mitgliedergruppen gemäß § 43 BerlHG[1] gerechnet werden.

Dieser Handlungsleitfaden betrachtet in erster Linie die Gegebenheiten bei der Auftragsdatenverarbeitung und berücksichtigt die Vereinbarungen der Freien Universität Berlin mit der Personalvertretung (§13 IT-Grundsatzdienstvereinbarung[8]). Auf allgemeine Aspekte der Fernwartung wird insoweit eingegangen, wie sie im Vorfeld eines Vertragsabschlusses geregelt werden können. In speziellen Situationen (beispielweise der (Fernzugriffs-)Support zur Fehlerbeseitigung durch nicht namentlich bekannte Mitarbeiter der Support-Firma), in denen eine detailierte vertragliche Regelung nicht möglich ist, sollen die Grundsätze dieses Leitfadens soweit wie möglich beachtet werden.

2 Aspekte des Zugriffs auf schützenswerte Daten

Beim Zugriff auf schützenswerte Daten der Freien Universität Berlin durch externe Personen ist eine Reihe von Gesetzen, Verordnungen und weiteren Regelungen zu beachten. Welche Regelungen im Einzelnen befolgt werden müssen, richtet sich vor allen Dingen nach der Art der Daten. In einer groben Unterscheidung können personenbezogene und nicht personenbezogene Daten getrennt betrachtet werden.

Abbildung 1: Vereinfachte Kategorisierung von schützenswerten Daten.

Bei den personenbezogenen Daten müssen stets die Vorschriften des Berliner Datenschutzgesetzes (BlnDSG) und ggf. des Bundesdatenschutzgesetzes (BDSG) beachtet werden. Spezielle Regelungen in Landesgesetzen, zum Beispiel §§ 6 bis 6 b BerlHG[1] oder § 91 LBG[6] ergänzen oder treten an die Stelle einzelner Paragraphen der Datenschutzgesetze. Dabei spielt es keine Rolle, ob es sich bei den personenbezogenen Daten um Daten von Mitgliedern der Freien Universität Berlin handelt oder nicht. Wenn es sich aber um Daten von Beschäftigten der Freien Universität Berlin handelt, müssen zusätzlich zu den Datenschutzgesetzen auch die Rechte der Personalvertretung nach dem Personalvertretungsgesetz und die in der IT-Grundsatzdienstvereinbarung festgelegten Regelungen berücksichtigt werden. Darüber hinaus können bei speziellen Daten noch weitere Sonderregelungen hinzukommen. Beispielsweise werden beim Betriebsärztlichen Dienst der Freien Universität Berlin Patientendaten verarbeitet, die einem besonderen Schutz unterliegen. Außerdem können Darstellungen wissenschaftlicher Daten dem Urheberrechtsgesetz (UrhG) unterliegen. Zu den geschützten Werken der Wissenschaft zählen nach § 2 Abs. 1 Nr. 7 UrhG[2] insbesondere Darstellungen wissenschaftlicher oder technischer Art, wie Zeichnungen, Pläne, Karten, Skizzen, Tabellen und plastische Darstellungen.

Entsprechend den verschiedenen Intentionen für einen Zugriff auf schützenswerte Daten der Freien Universität Berlin durch externe Personen müssen in den meisten Fällen folgende Regelungen beachtet werden:

- Auftragsdatenverarbeitung: Hierbei müssen insbesondere beachtet werden:

  - § 3 Berliner Datenschutzgesetz[3]
  - § 13 Dienstvereinbarung über die Grundsätze der Einführung und Anwendung Daten verarbeitender Systeme der Freien Universität Berlin (IT-Grundsatzdienstvereinbarung)[8]
  - § 12 IT-Grundsatzdienstvereinbarung[8] der Freien Universität Berlin
  - IT-Sicherheitsrichtlinie[7] der Freien Universität Berlin, insbesondere Abschnitt 2.2.2, Maßnahme M2.8
- Wartung bzw. Fernwartung durch externe Personen: Hierbei müssen insbesondere beachtet werden:
  - § 3a Berliner Datenschutzgesetz[3]
  - § 13 IT-Grundsatzdienstvereinbarung[8] der Freien Universität Berlin
  - IT-Sicherheitsrichtlinie[7] der Freien Universität Berlin, insbesondere Abschnitt 2.2.4, Maßnahme M2.23
- Softwareentwicklung durch externe Partner: Hierbei müssen insbesondere beachtet werden:
  - § 13 IT-Grundsatzdienstvereinbarung[8] der Freien Universität Berlin
  - IT-Sicherheitsrichtlinie[0] der Freien Universität Berlin

In der im Abschnitt 4 beschriebenen Checkliste wurden Maßnahmen zusammengestellt, die bei einem Zugriff auf schützenswerte Daten in der Regel zu beachten sind. Die Checkliste beinhaltet vor allen Dingen Maßnahmen, die entweder nicht gesetzlich geregelt oder in wenig bekannten Spezialgesetzen festgelegt sind. Welche der aufgeführten Punkte in welchem Umfang bzw. in welcher Ausprägung im konkreten Fall umgesetzt werden müssen, richtet sich nach dem Schutzbedarf und der Art der Daten. Der Schutzbedarf wird durch die Schutzbedarfsanalyse festgelegt und ist in der Verfahrensbeschreibung dokumentiert. Es ist davon auszugehen, dass die Checkliste die allermeisten Fälle berücksichtigt, dennoch kann keine Garantie auf Vollständigkeit gegeben werden. Daher muss in jedem Einzelfall geprüft werden, ob tatsächlich alle notwendigen Maßnahmen eingehalten werden und der Schutz der Daten gewährleistet ist.

Bereits bestehende IT-Verfahren bzw. (Fern-)Wartungsverträge, sollten von den zuständigen Verfahrensverantwortlichen daraufhin überprüft werden, ob ein Zugriff auf Daten der Freien Universität Berlin durch Externe erfolgt oder vorgesehen ist. Im Falle eines Datenzugriffs muss mit Hilfe des vorliegenden Handlungsleitfadens überprüft werden, ob alle notwendigen Vorkehrungen getroffen wurden, um die Sicherheit der Daten zu gewährleisten.

Die Maßnahmen, die sich aus der Checkliste für ein konkretes Projekt ergeben, müssen potenziellen Auftragnehmern frühzeitig bekannt gegeben werden. Insbesondere sollten diese Maßnahmen bei öffentlichen Ausschreibungen zusammen mit den anderen Verdingungsunterlagen veröffentlicht werden.

3 Workflow

In diesem Abschnitt wird die grundsätzliche Vorgehensweise bei einem geplanten Zugriff Externer auf Daten der Freien Universität Berlin dargestellt. Dabei werden zwei Fälle unterschieden. Im ersten Fall wird davon ausgegangen, dass im Zuge eines neuen Projekts noch keine Verträge oder sonstige Absprachen bestehen. Der zweite Fall berücksichtigt ein bereits bestehendes IT-Verfahren, in dem unter Umständen auch schon vertragliche Vereinbarungen existieren, in denen aber der Zugriff durch Externe noch nicht vorgesehen ist.

3.1 Neues Projekt bzw. Vorhaben

Sollen in einem Projekt oder in einem Vorhaben externe Personen bzw. Unternehmen auf Daten der Freien Universität Berlin zugreifen, soll nach dem folgenden Schema verfahren werden:

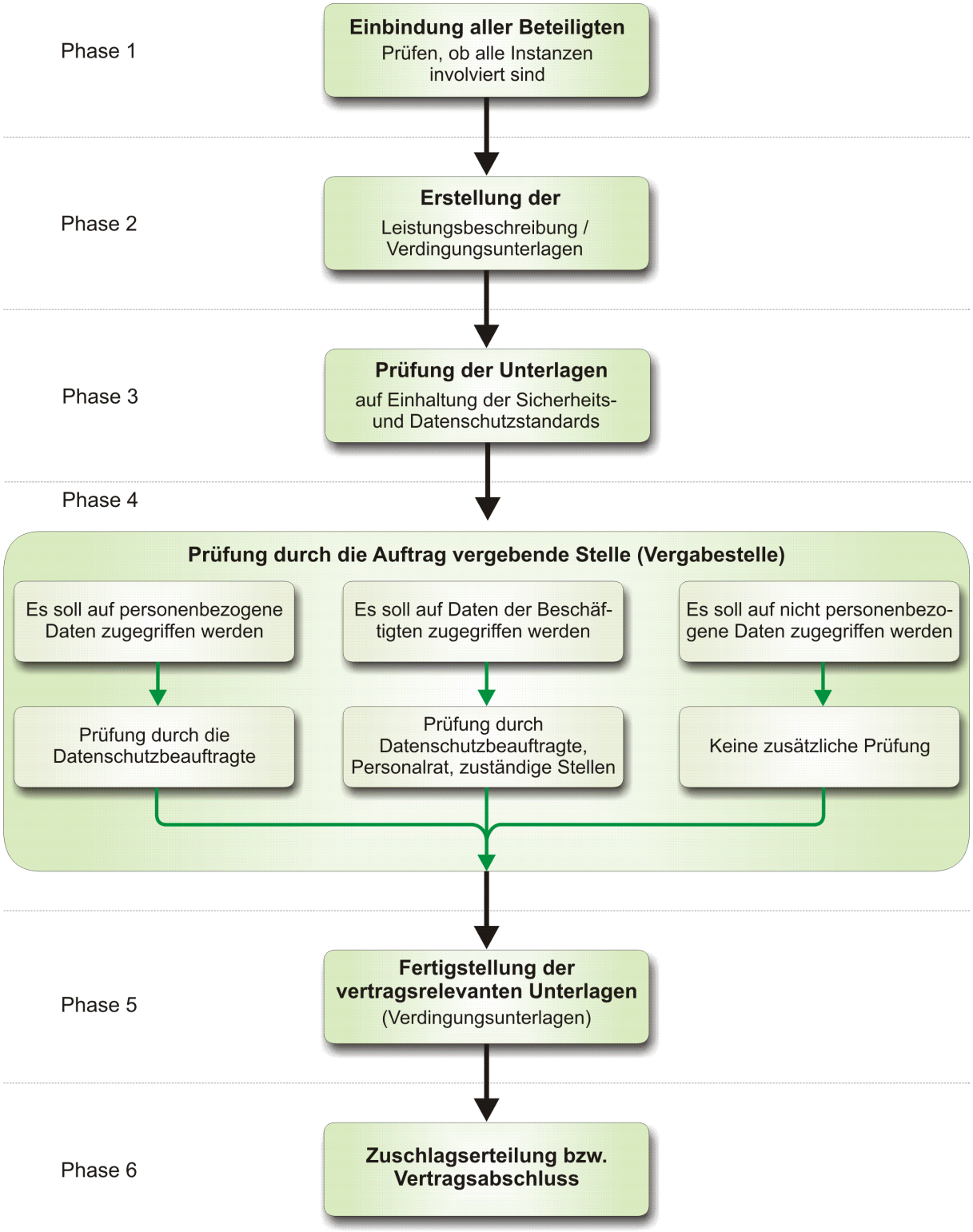

Abbildung 2: Schematische Darstellung des Workflows zur Erstellung der vertragsrelevanten Unterlagen.

3.1.1 Phase 1 – Einbindung aller Beteiligten

Es muss sichergestellt werden, dass von der verantwortlichen Stelle, die über den Datenzugriff entscheidet, alle Instanzen beteiligt werden. In jedem Fall muss der Dateneigner und/oder der Verfahrensverantwortliche involviert werden. Der Dateneigner ist für die Verarbeitung der Daten, auf die Externe zugreifen, verantwortlich. Der Verfahrensverantwortliche ist für die Durchführung einer Fachaufgabe bzw. die Erstellung eines Dienstes verantwortlich und ist in der Regel der Dateneigner. Er ist für alle IT-Aufgaben zuständig, die im Rahmen des von ihm verantworteten Verfahrens anfallen.

3.1.2 Phase 2 – Erstellung der Leistungsbeschreibung / Verdingungsunterlagen

Eine Leistungsbeschreibung (insbesondere ein Lastenheft) bzw. die Verdingungsunterlagen, die unter anderem den Zugriff auf schützenswerte Daten der Freien Universität Berlin durch externe Partner regeln, müssen unter Berücksichtigung der Checkliste gestaltet werden. Die Punkte in der Checkliste, die für den vorliegenden Fall relevant sind, müssen in geeigneter Form in den Text der Unterlagen aufgenommen werden. Als Hilfe für die Gestaltung der Unterlagen kann auf die Mustervereinbarung im Anhang dieses Leitfadens zurückgegriffen werden.

3.1.3 Phase 3 – Prüfung der Unterlagen auf Einhaltung der Sicherheits- und Datenschutzstandards

Die Verdingungsunterlagen müssen insbesondere auf Einhaltung der für den konkreten Fall relevanten Regelungen der Freien Universität Berlin (IT-Sicherheitsrichtlinie, IT-Grundsatzdienstvereinbarung usw.) und der gesetzlichen Bestimmungen (Berliner Datenschutzgesetz – BlnDSG) geprüft werden. Bei dieser Prüfung sind der Dateneigner bzw. der Verfahrensverantwortliche mit einzubeziehen.

3.1.4 Phase 4 – Prüfung durch die Auftrag vergebende Stelle (Vergabestelle)

Abhängig von der Art der Daten, auf die zugegriffen werden soll oder zugegriffen werden kann (Bsp. Wartung), leitet die Vergabestelle die Unterlagen zur weiteren Prüfung an die zuständigen Stellen weiter. Falls auf personenbezogene Daten zugegriffen werden soll, wird die Datenschutzbeauftragte um Begutachtung bzw. Stellungnahme gebeten. Falls es sich um personenbezogene Daten von Beschäftigten der Freien Universität Berlin handelt, werden darüber hinaus die Unterlagen zur Unterrichtung bzw. Beteiligung an den zuständigen Personalrat und den Dateneigner (i.d.R. Personalabteilung und – wenn Daten der Studierenden betroffen sind – Abteilung für Lehr- und Studienangelegenheiten) gesandt.

3.1.5 Phase 5 – Fertigstellung der vertragsrelevanten Unterlagen

Die Verdingungsunterlagen sind entsprechend den Hinweisen und Anmerkungen in den Prüfergebnissen zu bearbeiten. Falls die Vergabestelle, der Dateneigner und/oder der Verfahrensverantwortliche mit den Empfehlungen der prüfenden Stellen (Datenschutzbeauftragte, Personalrat usw. Personalabteilung) nicht einverstanden sind, werden die strittigen Punkte mit der betreffenden Stelle besprochen. Das Ziel dieser Besprechung ist eine einvernehmliche Lösung zu allen strittigen Punkten.

3.1.6 Phase 6 – Zuschlagserteilung bzw. Vertragsabschluss

Sobald die endgültige Fassung aller vertragsrelevanten Unterlagen vorliegt, kann es zum Vertragsabschluss kommen.

3.2 Bestehendes Projekt bzw. IT-Verfahren

Im Unterschied zu neuen IT-Verfahren bzw. Projekten, bei denen der Datenzugriff durch Externe von vornherein geplant ist, kann sich auch in bereits bestehenden IT-Verfahren im Nachhinein die Notwendigkeit eines Datenzugriffs durch Externe ergeben. In diesem Fall müssen die für das Verfahren relevanten Punkte der Checkliste beachtet werden. Der Zugriff auf schützenswerte Daten der Freien Universität Berlin durch externe Partner muss in jedem Fall auf eine vertragliche Grundlage gestellt werden. Insbesondere kann dies zur Folge haben, dass ein bestehender Vertrag zwischen der Freien Universität Berlin und externen Partnern modifiziert werden muss oder ein neuer Vertrag ausgearbeitet werden muss. Der Workflow entspricht im Prinzip dem Vorgehen in Abschnitt 3.1.1.

4 Checkliste

Die folgende Checkliste bezieht sich auf die Auftragsdatenverarbeitung. Sie ist für andere Verträge entsprechend anzuwenden.

Nr.	Beschreibung	Erfüllt	Nicht erfüllt	Trifft nicht zu
1.	Der Auftragnehmer wurde unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt. (§ 3 Abs. 1 BlnDSG[3] bei Auftragsdatenverarbeitung).*			
2.	Die für den konkreten Fall relevanten Regelungen der Freien Universität Berlin (IT-Sicherheitsrichtlinie, IT-Grundsatzdienstvereinbarung usw.) werden dem Auftragnehmer übergeben. Der Auftragnehmer verpflichtet sich, diese Regelungen im Rahmen des Vertragsverhältnisses zu berücksichtigen und einzuhalten.			
3.	Es werden jeweils schriftliche Aufträge in einer der folgenden Formen erteilt: • Einzelverträge oder • Rahmenverträge mit Einzelaufträgen (Einzelaufträge müssen hinreichend dokumentiert werden)			
4.	Die Personalvertretung wird so rechtzeitig vor der Vergabe des Auftrags bzw. vor Beginn des Vergabeverfahrens informiert, dass ggf. ein Mitwirkungs- oder Mitbestimmungsverfahren nach dem Landespersonalvertretungsgesetz durchgeführt werden kann.			
5.	Der Vertrag beinhaltet die genaue Bezeichnung des Vertragspartners.			
6.	Der Gegenstand des Vertragsverhältnisses ist genau beschrieben, besonders in Hinblick auf Art und Umfang der zu erbringenden Leistungen.			
7.	Im Vertrag sind technische und organisatorische Sicherungsmaßnahmen bei der Auftragsabwicklung vorzusehen, z.B. Protokollierung, Zugriffskontrolle, Umgang mit nicht mehr benötigten Arbeitsergebnissen.			
8.	Es wird eine Vereinbarung getroffen, die beinhaltet, dass der Auftraggeber das Recht hat, zur Erbringung von Leistungen Dritte heranzuziehen. Ggf. werden Unterauftragsverhältnisse festgelegt. Dabei muss sich der Auftragnehmer verpflichten, dass alle Regelungen, die für den Auftragnehmer gelten auch uneingeschränkt für Subunternehmer gelten.			

* Wie die Eignung geprüft wird, muss im Einzelfall festgelegt werden und hängt von mehreren Faktoren ab. Unter Umständen kann es ausreichen, wenn diese Maßnahmen in nachvollziehbarer und glaubhafter Weise dargelegt werden, in anderen Fällen muss ggf. eine weitergehende Überprüfung erfolgen. Auf jeden Fall ist hier ein sehr hoher Maßstab anzulegen, da die datenschutzrechtliche Verantwortung im Falle der Auftragsdatenverarbeitung bei der Freien Universität Berlin verbleibt.

Nr.	Beschreibung	Erfüllt	Nicht erfüllt	Trifft nicht zu
9.	Der Auftragnehmer wurde verpflichtet, die Vorschriften des Berliner Datenschutzgesetzes zu beachten.			
10.	Speicherungs- und Verarbeitungsort sowie die Art der Datenübermittlung sind genau beschrieben. Abhängig vom Ort der Datenverarbeitung hat sich der Auftragnehmer der Kontrolle der jeweils zuständigen Stelle zu unterwerfen. In diesem Fall wurde der Berliner Datenschutzbeauftragte informiert. (§3 Abs. 4 BlnDSG[3])			
11.	Der Vertrag beinhaltet Regelungen zur Gewährleistung der Sicherheit der Datenverarbeitung gemäß den Anforderungen des Berliner Datenschutzgesetzes (§ 5 Abs. 2 BlnDSG[3]). Insbesondere existierende Regelungen zu folgenden Punkten: Verantwortung, Art und Weise, schriftliche Bestätigung, Transportkontrolle sowie Protokollierung für den Datentransport. (Hinweis: Die Einhaltung muss regelmäßig kontrolliert werden.)			
12.	Die Plausibilitäts- und Sicherheitsprüfungen beim Dateneingang durch den Auftragnehmer sind genau definiert.			
13.	Es werden Vereinbarungen zu Laufzeiten und Kündigungsfristen getroffen.			
14.	Pflichten, die über das Vertragsende hinausreichen, sind genau beschrieben.*			
15.	Die Weisungs- und Kontrollrechte des Auftraggebers / Auftragnehmers sind genau definiert. Insbesondere sind alle Kommunikationspartner benannt bzw. im Falle nicht einzeln benennbarer Personen (z. B. die Entwicklungsabteilung eines großen Auftragnehmers), der Kreis der Kommunikationspartner genau definiert.			
16.	Der Auftraggeber wird bei Störungen rechtzeitig unterrichtet.			
17.	Die Mitarbeiter des Auftragsnehmers werden auf das Datengeheimnis verpflichtet.			
18.	Die Aufbewahrungsdauer der Datenbestände und der Software beim Auftragnehmer wird festgelegt.			
19.	Der Auftragnehmer weist die ordnungsgemäßen Berichtigungs-, Sperrungs- und Löschungsmöglichkeiten nach.			
20.	Der Auftraggeber hat das Recht zur sofortigen Kündigung bei Nichtbeachtung von Verpflichtungen (evtl. Vertragsstrafen)**			
21.	Im Falle gesetzlicher Offenbarungspflichten des Auftragnehmers muss der Auftraggeber benachrichtigt werden. Dies ist in geeigneter Weise festzulegen.			

* Welche Pflichten über eine Beendigung des Vertrags fortgelten ist abhängig vom Einzelfall.

** Die Art der Vorkommnisse, die so gravierend sind, dass der Auftraggeber das Recht zur sofortigen Kündigung hat, ist stets vom Einzelfall abhängig. In der Regel sollte vor einer sofortigen Kündigung eine schriftliche Aufforderung mit Fristsetzung erfolgen.

5 Anlage: Mustervereinbarung für Auftragsdaten-verarbeitung

Die nachfolgende Mustervereinbarung als Ergänzung zum Vertragstext soll als Hilfe und Orientierung dienen, mit Auftragnehmern ausreichende vertragliche Regelungen unter Beachtung des Berliner Datenschutzgesetzes, universitätsinterner Regelungen und eventueller sonstiger spezialgesetzlicher Bestimmungen zu vereinbaren. Spezielle Anforderungen des Einzelfalls müssen in dem Vereinbarungsentwurf entsprechend berücksichtigt werden. Im Rahmen öffentlicher Ausschreibungen sollte diese (oder eine ähnliche) Vereinbarung zusammen mit den anderen Verdingungsunterlagen veröffentlicht werden.

Vereinbarung

zwischen dem/der

.....

– nachstehend Auftragnehmer genannt –

und der

Freien Universität Berlin – nachstehend Auftraggeber genannt –

wird folgende Vereinbarung getroffen:

§ 1 Gegenstand der Vereinbarung

(1) Der Auftragnehmer verarbeitet schützenswerte Daten im Auftrag des Auftraggebers. [*Hinweis: Die schützenswerten Daten sind genau zu bezeichnen.*]

(2) Der Schutzbedarf der Daten wird durch das Ergebnis der in der IT-Sicherheitsrichtlinie der Freien Universität Berlin beschriebenen Schutzbedarfsanalyse bestimmt. Als schützenswert gelten insbesondere alle personenbezogenen Daten.

(3) Der Auftragnehmer verpflichtet sich zur Einhaltung und Umsetzung aller dem Schutzbedarf der Daten angemessenen Maßnahmen. Die Art und Weise der Umsetzung richtet sich nach den gesetzlichen Vorgaben und den an der Freien Universität Berlin geltenden Richtlinien und Vereinbarungen.

§ 2 Pflichten

(1) Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich.

(2) Für die vereinbarte Datenverarbeitung gelten an der Freien Universität Berlin folgende Regelungen:

- IT-Sicherheitsrichtlinie der Freien Universität Berlin
- …[*Hinweis: Weitere Regelwerke sind zu ergänzen.*]

Der Auftragnehmer verpflichtet sich, im Rahmen der Vereinbarung, diese Regelungen einzuhalten und zu befolgen.

(3) Der Auftragnehmer verarbeitet vorbezeichnete Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers. Er verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen Zwecke. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt.

(4) Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von schützenswerten Daten die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die verarbeiteten Daten von sonstigen Datenbeständen getrennt werden.

(5) Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber jederzeit berechtigt ist, die Einhaltung der Regeln zur IT-Sicherheit und der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie -vorgänge.

(6) Nicht mehr benötigte Unterlagen mit schützenswerten Daten und Dateien dürfen erst nach vorheriger Zustimmung durch den Auftraggeber datenschutzgerecht vernichtet werden.

(7) Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen. Die Datenträger des Auftragnehmers sind danach physisch zu löschen. Test- und Ausschussmaterial ist unverzüglich zu vernichten oder dem Auftraggeber auszuhändigen.

[*1. Alternative*]

(8) Die Einschaltung von Subauftragnehmern ist ausgeschlossen.

[*2. Alternative*]

(8) Die Beauftragung von Subunternehmen ist nur mit schriftlicher Zustimmung des Auftraggebers zugelassen. Der Auftragnehmer hat in diesem Falle vertraglich sicherzustellen, dass die vereinbarten Regelungen auch gegenüber Subunternehmern gelten. Er hat die Einhaltung dieser Pflichten regelmäßig zu überprüfen. Die Weiterleitung von Informationen und/oder Daten ist erst zulässig, wenn der Subunternehmer die Verpflichtung nach § 4 erfüllt hat.

(9) Soweit für den Auftragnehmer die datenschutzrechtlichen Vorschriften über den nichtöffentlichen Bereich Anwendung finden, bestätigt er durch Vorlage der erforderlichen Meldeunterlagen, dass er zum Register bei der zuständigen Aufsichtsbehörde für den Datenschutz gemeldet ist. Die Datenschutzmeldung wird dem Auftraggeber in der aktuellen Fassung zugänglich gemacht. Wird die Meldung nicht bei der Aufsichtsbehörde geführt, gibt der Auftragnehmer dem Auftraggeber die Kontaktdaten seines Datenschutzbeauftragten bekannt.

(10) Für die Sicherheit erhebliche notwendige Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind mit dem Auftraggeber abzustimmen.

§ 3 Datengeheimnis

(1) Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers das Datengeheimnis gemäß § 8 Berliner Datenschutzgesetz (BlnDSG) zu wahren. Er verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen (§ 3 Abs. 4 BlnDSG). Die Wahrung des Datengeheimnisses ist auch auf alle nicht personenbezogenen schützenswerten Daten in entsprechender Form anzuwenden.

(2) Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Der Auftragnehmer sichert zu, dass die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter auf das Datengeheimnis gemäß § 8 BlnDSG verpflichtet wurden.

(3) Auskünfte darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

§ 4 Kontrollrechte des Berliner Beauftragten für Datenschutz und Informationsfreiheit

(1) Der Auftragnehmer verpflichtet sich, dem Berliner Beauftragten für Datenschutz und Informationsfreiheit und den von ihm beauftragten Bediensteten Zugang zu den Arbeitsräumen zu gewähren und unterwirft sich der Kontrolle nach Maßgabe des BlnDSG in seiner jeweiligen Fassung. Findet die Datenverarbeitung in einem anderen Bundesland oder in einem anderen Mitgliedsstatt der EU statt, unterwirft sich der Auftragnehmer der Kontrolle der jeweils zuständigen Stelle.

§ 5 Datensicherungsmaßnahmen

(1) Der Auftragnehmer verpflichtete sich zur Umsetzung aller technischen und organisatorischen Maßnahmen, die den Anforderungen nach § 5 BlnDSG sowie den der IT-Sicherheitsrichtlinie der Freien Universität Berlin genügen.

(2) An der Erstellung der Vorabkontrolle gem. § 5 BlnDSG Abs. 3 und der Verfahrensbeschreibungen gemäß der in der IT-Grundsatzdienstvereinbarung der Freien Universität Berlin festgelegten Kriterien hat der Auftragnehmer mitzuwirken. Er hat die erforderlichen Angaben dem Auftraggeber zuzuleiten.

(3) Der Auftragnehmer beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung. Er gewährleistet die vertraglich vereinbarten und gesetzlich vorgeschriebenen Datensicherheitsmaßnahmen.

(4) Die technischen und organisatorischen Maßnahmen können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden. Wesentliche Änderungen werden schriftlich vereinbart.

(5) Soweit die beim Auftragnehmer getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich nach seiner Kenntnisnahme. Entsprechendes gilt für Störungen sowie bei Verdacht auf Da-

tenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung schützenswerter Daten.

(6) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn eine vom Auftraggeber erteilte Weisung nach seiner Meinung zu einem Verstoß gegen gesetzliche Vorschriften führen kann. Die Weisung braucht nicht befolgt zu werden, solange sie nicht durch den Auftraggeber geändert oder ausdrücklich bestätigt wird.

§ 6 Dauer der Vereinbarung

Diese Vereinbarung ist an die Laufzeit des zugrundliegenden Vertrags gekoppelt. Hiervon ausgenommen sind Regelungen, die dem Schutz der Daten dienen. Sie gelten solange wie der Schutzbedarf der Daten besteht.

§ 7 Strafe bei Nichteinhaltung der Regelungen dieser Vereinbarung

Bei Verstoß gegen die Abmachungen dieser Vereinbarung, insbesondere gegen die Einhaltung des Datenschutzes, gelten die im Vertragswerk vereinbarten Vertragsstrafen.

§ 8 Sonstiges

Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

§ 9 Wirksamkeit der Vereinbarung

(1) Die Unwirksamkeit einer Vereinbarungsregelung berührt die Gültigkeit der übrigen Regelungen nicht. Sollte sich eine Regelung als unwirksam erweisen, wird diese durch eine neue ersetzt, die dem Gewollten am nächsten kommt.

(2) Änderungen dieser Vereinbarung bedürfen der Schriftform.

(3) Für Nebenabreden ist die Schriftform erforderlich.

(4) Diese Vereinbarung unterliegt ausschließlich deutschem Recht. Sofern der Auftragnehmer ein Kaufmann, eine juristische Person des öffentlichen Rechts oder ein öffentlich-rechtliches Sondervermögen ist oder keinen allgemeinen Gerichtsstand im Inland hat, wird Berlin als ausschließlicher Gerichtsstand für alle Streitigkeiten aus und in Zusammenhang mit dieser Vereinbarung vereinbart. Dies gilt nicht, soweit ein ausschließlicher Gerichtsstand gesetzlich vorgeschrieben ist.

6 Verzeichnis der zitierten Gesetze

1. Gesetz über die Hochschulen im Land Berlin; **Berliner Hochschulgesetz – BerlHG** in der Fassung des Elften Änderungsgesetzes vom 6. Juli 2006

2. Gesetz über Urheberrecht und verwandte Schutzrechte (**Urheberrechtsgesetz – UrhG**) vom 9. September 1965 (BGBl. I S. 1273), zuletzt geändert durch Artikel 6 des Gesetzes vom 7. Juli 2008 (BGBl. I S. 1191)"

3. Gesetz zum Schutz personenbezogener Daten in der Berliner Verwaltung (**Berliner Datenschutzgesetz – BlnDSG**) in der Fassung vom 17. Dezember 1990 (GVBl. 1991 S. 16, 54), zuletzt geändert durch Gesetz vom 30. November 2007 (GVBl. S. 598)

4. **Bundesdatenschutzgesetz (BDSG)** in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Artikel 1 des Gesetzes vom 22. August 2006 (BGBl. I S. 1970)

5. **Landespersonalvertretungsgesetz (LPersVG)** Berlin in der Fassung vom 17. Juli 2008

6. **Landesbeamtengesetz (LBG)** Berlin in der Fassung vom 19. März 2009

7. **IT-Sicherheitsrichtlinie** der Freien Universität Berlin; bekanntgegeben durch Rundschreiben Serie V, Nr. 05/2008 vom 25. Juni 2008

8. Dienstvereinbarung über die Grundsätze der Einführung und Anwendung Daten verarbeitender Systeme an der Freien Universität Berlin (**IT-Grundsatzdienstvereinbarung**) vom 05. Dezember 2008