Kooperationsvereinbarung der Thüringer Hochschulen für IT-Dienste

Präambel

Die Hochschulen im Freistaat Thüringen gemäß § 1 Abs. 2 ThürHG werden, ausgehend von der Forderung in § 5 Absatz 7 ThürHG bei ihrer Aufgabenwahrnehmung die Zusammenarbeit zu vertiefen, ihre Kooperation im Bereich der Erbringung von IT-Diensten erweitern und verstärken. Hierzu schließen sie die nachfolgende Vereinbarung, mit der die Grundsätze der Zusammenarbeit einvernehmlich festgeschrieben werden.

Grundsatz der Kooperation

Die Hochschulen gehen die Kooperation im gegenseitigen Vertrauen auf die bestmögliche Unterstützung der Geschäftsprozesse der Einrichtungen ein. Die Mitarbeiter der jeweiligen IT-Servicezentren (Rechenzentren) arbeiten unmittelbar zusammen, die Steuerung obliegt den jeweiligen Leitern dieser Einrichtungen.

Die Hochschulleitungen sind über den zentralen IT-Dienstleister der Hochschule einzubeziehen, wenn neue Dienste in Kooperation erbracht werden sollen, eine Kooperation teilweise bzw. ganz beendet wird oder andere wesentliche Änderungen eintreten.

Vertraulichkeit, Auftragsdatenverarbeitung, Datenschutz

Die Hochschulen sichern sich im Umgang mit den Daten gegenseitig dieselbe Sorgfalt zu wie innerhalb der eigenen Hochschule. Die Hochschulen verpflichten sich, die Vertraulichkeit von geheimhaltungsbedürftigen Informationen und personenbezogenen Daten zu wahren und ohne Zustimmung der betroffenen Hochschule keine Informationen oder Daten preiszugeben, es sei denn, es besteht eine gesetzliche Pflicht. In diesem Fall ist die betroffene Hochschule rechtzeitig zu informieren. Im Übrigen gelten für die Verarbeitung personenbezogener Daten die Bestimmungen des Thüringer Datenschutzgesetzes in der jeweils geltenden Fassung.

Sofern bei der Erbringung von IT-Diensten personenbezogene Daten zu verarbeiten sind, werden die Daten verschiedener Hochschulen in der Regel voneinander getrennt verarbeitet. Über begründete Ausnahmen entscheiden die Leiter der beteiligten Rechenzentren unter Beteiligung der Datenschutzbeauftragten.

Die Hochschulen verpflichten ihre Mitarbeiter und alle eingebundenen Dienstleister zur gewissenhaften Erfüllung der sich hieraus ergebenden Obliegenheiten, insbesondere tragen sie dafür Sorge, dass die Mitarbeiter entsprechend belehrt werden.

Die Einbeziehung Dritter bei der Erbringung von IT-Diensten ist nur zulässig, wenn diese zur Einhaltung der Pflichten nach dieser Vereinbarung und den geltenden Datenschutzgesetzen verpflichtet werden.

Die Verfahrensverantwortung und die Verantwortung für die Einhaltung gesetzlicher Bestimmungen verbleiben jeweils bei der auftraggebenden Hochschule, es sei denn, dass sich aus Gesetz oder dieser Vereinbarung etwas anderes ergibt. Die Haftung der Hochschule, die eine IT-Dienstleistung erbringt, ihrer gesetzlichen Vertreter sowie ihrer

Erfüllungs- und Verrichtungsgehilfen beschränkt sich auf Vorsatz und grobe Fahrlässigkeit. Ein Schadensersatz für Folgeschäden oder entgangenen Gewinn ist ausgeschlossen.

Die Rahmendaten zu einem IT-Dienst werden in der Regel jeweils gemäß der Anlage zu dieser Vereinbarung erfasst und sind damit Bestandteil dieser Vereinbarung. Soweit es sich um Auftragsdatenverarbeitung iSv § 8 ThürDSG handelt, gelten, soweit zwischen den Hochschulen nichts anderes vereinbart wird, die Bestimmungen der Rahmenvereinbarung zur Auftragsdatenverarbeitung, die als Anlage Vertragsbestandteil ist.

Bekanntmachung

Die Hochschulen setzen die jeweils zu beteiligenden Einrichtungen (IT-Dienstleister, Personalrat, Datenschutzbeauftragte o.ä.) von dieser Vereinbarung in Kenntnis und beteiligen diese im erforderlichen Ausmaß.

Schlussbestimmungen

Die Kooperation wird auf unbestimmte Zeit geschlossen.

Die Hochschulen tauschen sich regelmäßig über den Stand der Kooperation aus. Sie verpflichten sich, Fragen im Zusammenhang mit dieser Kooperation einvernehmlich zu klären.

Wird diese Kooperation einvernehmlich beendet oder tritt eine Hochschule aus der Kooperation aus, besteht die Pflicht zur Vertraulichkeit von geheimhaltungsbedürftigen Informationen und personenbezogenen Daten, die aufgrund dieser Kooperation erlangt wurden, fort.

Anlagen:

- Rahmenvereinbarung zur Auftragsdatenverarbeitung
- Rahmendaten für die Kooperation bei der Erbringung von IT-Diensten

UNIVERSITÄT ERFURT

Erfurt, den

Prof. Dr. Walter Bauer-Wabnegg
Präsident

Jan Gerken
Kanzler

FACHHOCHSCHULE ERFURT UNIVERSITY OF APPLIED SCIENCES

Erfurt, den

Prof. Dr. Volker Zerbe
Rektor

Marion Britta Werner
Kanzlerin

TECHNISCHE UNIVERSITÄT ILMENAU

Ilmenau, den

Prof. Dr. Peter Scharff
Rektor

Dr. Margot Bock
Kanzlerin

seit 1558

Jena, den

Prof. Dr. Walter Rosenthal
Präsident

Dr. Klaus Bartholmé
Kanzler

Ernst-Abbe-Hochschule Jena
University of Applied Sciences

Jena, den

Prof. Dr. Gabriele Beibst
Rektorin

Dr. Thoralf Held
Kanzler

HOCHSCHULE NORDHAUSEN
University of Applied Sciences

Nordhausen, den

Prof. Dr. Jörg Wagner
Präsident

Hans-Wolfgang Köllmann
Kanzler

HOCHSCHULE SCHMALKALDEN
UNIVERSITY OF APPLIED SCIENCES

Schmalkalden, den

Prof. Dr. Elmar Heinemann
Rektor

Thomas Losse
Kanzler

Bauhaus-Universität Weimar

Weimar, den

Prof. Dr. Karl Beucke
Rektor

Dr. Horst Henrici
Kanzler

Weimar, den

Prof. Dr. Christoph Stölzl
Präsident

Christine Gurk
Kanzlerin

Anlage

Kooperation bei der Erbringung von IT-Diensten

IT-Dienst / IT-unterstütztes Verfahren	
Stand / Version	
Kurzbeschreibung	
Auftraggeber (verfahrensverantwortliche Hochschule und Organisationseinheit)	
Verfahrensverantwortliche(r)*	
Dienste-Erbringer (Hochschule bzw. IT-Dienstleistungszentrum)	
Verantwortliche(r)* des IT-Dienste-Erbringers	
Eingesetzte Hard- und Software bis zum Zeitpunkt der Vereinbarung	
Übertragene Daten	

*Der Verfahrensverantwortliche ist bzgl. der verarbeiteten Daten seiner Hochschule gegenüber den Mitarbeitern des IT-Dienstleisters weisungsbefugt.
Es sind jeweils die Funktion und der Name einzutragen.

Rahmenvereinbarung zur Auftragsdatenverarbeitung

zwischen den Thüringer Hochschulen

Universität Erfurt
Fachhochschule Erfurt
Technische Universität Ilmenau
Friedrich-Schiller-Universität Jena
Ernst-Abbe-Hochschule Jena
Hochschule Nordhausen
Hochschule Schmalkalden
Bauhaus Universität Weimar
Hochschule für Musik FRANZ LISZT Weimar

Präambel

Die Hochschulen im Freistaat Thüringen gemäß § 1 Abs. 2 ThürHG werden, ausgehend von der Forderung in § 5 Absatz 7 ThürHG bei ihrer Aufgabenwahrnehmung die Zusammenarbeit zu vertiefen, ihre Kooperation im Bereich der Erbringung von IT-Diensten erweitern und verstärken. Hierzu haben sie eine Kooperationsvereinbarung geschlossen, mit der die Grundsätze der Zusammenarbeit einvernehmlich festgeschrieben werden. Im Rahmen dieser Zusammenarbeit erbringen aufgrund der technischen Bedingungen und Ressourcen (insb. zentrale, landesweite oder hochschulübergreifende Dienste u. ä.) einzelne Hochschulen Dienste für andere Hochschulen. Dabei können auch personenbezogene Daten einer Hochschule durch eine andere Hochschule verarbeitet werden. Soweit es sich hierbei um eine Auftragsdatenverarbeitung i. S. v. § 8 ThürDSG handelt, gewährleisten die Hochschulen die Einhaltung der maßgeblichen datenschutzrechtlichen Bestimmungen gemäß dem Thüringer Datenschutzgesetz. Zur Umsetzung schließen sie diese Rahmenvereinbarung und verpflichten sich gegenseitig, die nachfolgenden Bestimmungen zu beachten.

§ 1 Gegenstand der Rahmenvereinbarung

(1) Diese Vereinbarung regelt die Verarbeitung personenbezogener Daten einer Thüringer Hochschule gemäß § 1 Abs. 2 ThürHG durch eine andere Thüringer

Hochschule. Soweit es sich hierbei um eine Auftragsdatenverarbeitung handelt, ist die datenverarbeitende Hochschule Auftragnehmerin i. S. v. § 8 ThürDSG und die Hochschule, deren Daten verarbeitet werden, Auftraggeberin i. S. v. § 8 ThürDSG. Sofern sie danach Auftraggeberin oder Auftragnehmerin sind, sind die jeweiligen Pflichten nach dieser Vereinbarung zu beachten.

(2) Diese Vereinbarung kann durch gesondert abzuschließende Einzelvereinbarungen ergänzt werden, wenn es die Besonderheiten des Verfahrens erfordern oder eine Hochschule dies wünscht. In einer Einzelvereinbarung zu dieser Rahmenvereinbarung können insbesondere enthalten sein:

- der Gegenstand des Auftrags/die Aufgaben,
- der Umfang und der Zweck der Datenverarbeitung oder -nutzung,
- die Kostentragung der bei der Auftragnehmerin zusätzlich entstehenden Kosten.

Änderungen der Auftragsinhalte sind zwischen den jeweiligen Hochschulen abzustimmen.

§ 2 Pflichten einer Hochschule als Auftraggeberin

(1) Für die Beurteilung der Zulässigkeit der Datenverarbeitung und -nutzung sowie für die Wahrung der Rechte der Betroffenen ist allein die Auftraggeberin verantwortlich.

(2) Die Auftraggeberin kann Weisungen über Art, Umfang und Verfahren der Datenverarbeitung erteilen; mündliche Weisungen sind auf Verlangen unverzüglich schriftlich zu bestätigen.

(3) Die Auftraggeberin informiert die Auftragnehmerin unverzüglich, wenn sie Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

§ 3 Pflichten einer Hochschule als Auftragnehmerin

(1) Die Auftragnehmerin verarbeitet und/oder nutzt personenbezogene Daten bzw. schutzbedürftige Informationen ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung der Auftraggeberin. Sie verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen Zwecke. Kopien oder Duplikate werden ohne Genehmigung der Auftraggeberin nicht erstellt, soweit diese nicht zur Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage erforderlich sind. Die zu verarbeitenden Daten werden in der Regel von sonstigen Datenbeständen zumindest logisch getrennt verarbeitet; Ausnahmen können unter Beteiligung der Datenschutzbeauftragten vereinbart werden. Die Auftragnehmerin hat personenbezogene Daten, die sich auf ihrem IT-System befinden, zu berichtigen, zu sperren oder zu löschen, wenn die Auftraggeberin dies in der getroffenen Vereinbarung oder einer Weisung verlangt.

(2) Verlangt ein Dritter oder ein Betroffener die Herausgabe bzw. die Bekanntgabe von Daten, die im Rahmen der Auftragsdatenverarbeitung verarbeitet bzw. genutzt

werden, leitet die Auftragnehmerin diesbezügliche Begehren an die Auftraggeberin weiter.

(3) Die Verarbeitung von personenbezogenen Daten außerhalb der Geschäftsräume der Auftragnehmerin, insbesondere in Privatwohnungen, ist nur zulässig, soweit dies im Rahmen einer Einzelvereinbarung gestattet wird.

(4) Die Auftragnehmerin hat an der Erstellung des Verfahrensverzeichnisses mitzuwirken. Sie hat der Auftraggeberin die erforderlichen Angaben zuzuleiten. Sie erklärt sich ferner damit einverstanden, dass die Auftraggeberin jederzeit berechtigt ist, die Einhaltung 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, die Einsichtnahme in Unterlagen, die Vorführung der im Rahmen der Auftragsdatenverarbeitung umgesetzten betrieblichen Abläufe sowie sonstige Kontrollen vor Ort. Die Auftragnehmerin unterrichtet die Auftraggeberin umgehend bei Prüfungen durch die Aufsichtsbehörden.

(5) Nach Abschluss der vertraglichen Arbeiten, ggf. einschließlich gesetzlicher Aufbewahrungsfristen, hat die Auftragnehmerin sämtliche in ihren Besitz gelangten Unterlagen und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, der Auftraggeberin auszuhändigen. Die Datenträger der Auftragnehmerin sind danach physisch zu löschen. Test- und Ausschussmaterial sowie Datensicherungskopien sind unverzüglich nach Abschluss der vertraglichen Arbeiten der Auftraggeberin auszuhändigen oder irreversibel zu löschen. Soweit für die Löschung weitergehende Anforderungen zu beachten sind, ist dies in der Einzelvereinbarung festzulegen. Für die Maßnahmen dieses Absatzes dürfen durch die Auftragnehmerin Kosten nur dann geltend gemacht werden, wenn dies in einer Einzelvereinbarung vorgesehen ist.

(6) Die Auftragnehmerin beachtet die Grundsätze ordnungsmäßiger Datenverarbeitung. Sie gewährleistet die gesetzlich vorgeschriebenen und vertraglich vereinbarten Datensicherheitsmaßnahmen. Soweit die Auftragnehmerin der Ansicht ist, dass eine Weisung der Auftraggeberin gegen das ThürDSG oder andere Vorschriften über den Datenschutz verstößt, hat sie die Auftraggeberin unverzüglich darauf hinzuweisen.

§ 4 Datengeheimnis und Vertraulichkeit

(1) Die diese Vereinbarung schließenden Hochschulen verpflichten sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten das Datengeheimnis gemäß § 6 ThürDSG zu wahren.

(2) Sie verpflichten sich ferner, alle im Rahmen der Auftragsverhältnisse erlangten Kenntnisse von als vertraulich gekennzeichneten Informationen der Hochschulen vertraulich zu behandeln.

(3) Die Hochschulen informieren sich unverzüglich gegenseitig über sie betreffende Störungen oder Verstöße gegen datenschutzrechtliche Bestimmungen sowie bei Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten.

§ 5 Datensicherungsmaßnahmen

Die technischen und organisatorischen Maßnahmen nach § 9 ThürDSG werden in der Anlage TOM festgelegt, die Bestandteil dieses Vertrages ist. In einer Einzelvereinbarung können Abweichungen festgelegt werden, soweit dies im Einzelfall geboten ist. Die Wirksamkeit der technischen und organisatorischen Maßnahmen ist unter Berücksichtigung sich verändernder Rahmenbedingungen und der Entwicklung der Technik regelmäßig zu überprüfen. Die sich daraus ergebenden notwendigen Anpassungen sind mit der Auftraggeberin abzustimmen und gegebenenfalls in die Einzelvereinbarung aufzunehmen.

§ 6 Haftung

(1) Die Hochschulen haften einander für Schäden, die bei der Erbringung der vertraglichen Leistung vorsätzlich oder grob fahrlässig verursacht werden. Der Ersatz für entgangenen Gewinn oder Folgeschäden ist ausgeschlossen.

(2) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach dem ThürDSG oder anderen Vorschriften für den Datenschutz unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, ist die Auftraggeberin gegenüber den Betroffenen verantwortlich. Soweit die Auftraggeberin zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihr der Rückgriff bei der Auftragnehmerin vorbehalten.

§ 7 Schlussbestimmungen

(1) Diese Rahmenvereinbarung tritt mit ihrer Unterzeichnung in Kraft und wird auf unbestimmte Zeit geschlossen.

(2) Wird diese Kooperation einvernehmlich beendet oder tritt eine Hochschule aus der Kooperation aus, besteht die Pflicht zur Vertraulichkeit von geheimhaltungsbedürftigen Informationen und personenbezogenen Daten, die aufgrund dieser Kooperation erlangt wurden, fort.

(3) Die Hochschulen bemühen sich, Fragen im Zusammenhang mit dieser Vereinbarung einvernehmlich zu klären. Änderungen und Ergänzungen dieser Rahmenvereinbarung und der Einzelvereinbarungen bedürfen der Schriftform. Dies gilt auch für die Änderung des Schriftformerfordernisses.

(4) Wird bei der Aufgabenerfüllung ein Dritter einbezogen, hat die jeweilige Hochschule sicher zu stellen, dass die Verpflichtungen nach dieser Vereinbarung auch für den Dritten gelten.

(5) Die Hochschulen informieren sich gegenseitig über wesentliche Änderungen in der Organisation und bei der Durchführung der Datenverarbeitung, soweit dies auf die jeweilige Aufgabenerfüllung Auswirkungen hat.

Anlage: Technische und organisatorische Maßnahmen (TOM)

UNIVERSITÄT ERFURT

Erfurt, den

Prof. Dr. Walter Bauer-Wabnegg
Präsident

Jan Gerken
Kanzler

FACHHOCHSCHULE ERFURT UNIVERSITY OF APPLIED SCIENCES

Erfurt, den

Prof. Dr. Volker Zerbe
Rektor

Marion Britta Werner
Kanzlerin

TECHNISCHE UNIVERSITÄT ILMENAU

Ilmenau, den

Prof. Dr. Peter Scharff
Rektor

Dr. Margot Bock
Kanzlerin

seit 1558

Jena, den

Prof. Dr. Walter Rosenthal
Präsident

Dr. Klaus Bartholmé
Kanzler

Ernst-Abbe-Hochschule Jena
University of Applied Sciences

Jena, den

Prof. Dr. Gabriele Beibst
Rektorin

Dr. Thoralf Held
Kanzler

HOCHSCHULE NORDHAUSEN
University of Applied Sciences

Nordhausen, den

Prof. Dr. Jörg Wagner
Präsident

Hans-Wolfgang Köllmann
Kanzler

HOCHSCHULE SCHMALKALDEN
UNIVERSITY OF APPLIED SCIENCES

Schmalkalden, den

Prof. Dr. Elmar Heinemann
Rektor

Thomas Losse
Kanzler

Bauhaus-Universität Weimar

Weimar, den

Prof. Dr. Karl Beucke
Rektor

Dr. Horst Henrici
Kanzler

Weimar, den

Prof. Dr. Christoph Stölzl
Präsident

Christine Gurk
Kanzlerin

Anlage

Technische und organisatorische Maßnahmen (TOM)

Gemäß § 9 Abs. 2 ThürDSG sollen die technischen und organisatorischen Maßnahmen (TOM) Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit und Transparenz gewährleisten. Dazu muss der Schutzbedarf und daraus folgend der Handlungsbedarf für den konkreten Einzelfall ermittelt werden. Die Verantwortung hierfür liegt bei den Stellen, die die Rahmen- bzw. Einzelvereinbarung abschließen.

Bei einem niedrigen bis mittleren Schutzbedarf werden die folgenden Maßnahmen in vielen Fällen notwendig aber auch ausreichend sein.

1. Befugnis und Rechtevergabe
    a. Nur Befugte erhalten Zugang zu personenbezogenen Daten.
    b. Die Befugnis ergibt sich aus einer individuellen, personenbezogenen Rechtevergabe an die betreffenden Personen durch die Vertragspartei.
    c. Die Rechtevergabe erfolgt nur soweit und solange diese zur Erfüllung der Aufgaben der betreffenden Person erforderlich ist.
    d. Die Kompetenz zur Rechtevergabe sowie zu den einzelnen Vergaben, Entziehungen und Änderungen von Rechten sowie das Verfahren an sich sind zu dokumentieren.

2. Schutz der IT-Infrastruktur
    a. Die IT-Infrastruktur ist angemessen zu sichern. Insbesondere sollen Serverräume über einen Brandschutz und eine Raumüberwachung sowie eine angemessene Einbindung in die Versorgung der Hochschule mit Strom und Abwärme verfügen.
    b. Die IT-Infrastruktur (Server, Rechner, Netze) ist durch hardware- und softwareseitige Maßnahmen, z.B. Firewalls, Scanner gegen Viren und Schadsoftware gegen Zugriffe Unbefugter, zu schützen.
    c. Für die Datenverarbeitung benötigte Server befinden sich ausschließlich in alarmgesicherten Räumen, die gegen unbefugten Zutritt gesichert sind. Die Sicherung gegen unbefugten Zutritt erfolgt zumindest entweder durch elektronische Zugangskontrollen oder ein Schließsystem, bei dem nachvollzogen werden kann, wer wann welchen Schlüssel erhalten und zurückgegeben hat.
    d. Die Übertragung personenbezogener Daten erfolgt durch verschlüsselte Verfahren.
    e. Auch befugte Personen erlangen nur Zugriff auf personenbezogene Daten nach Autorisierung und Authentifizierung.
    f. Die Autorisierung erfolgt mittels Benutzerkennungen, die für Dritte nicht offenkundig sind (z.B. keine Identität mit dem Namen des Benutzers oder der allgemein bekannten E-Mail-Adresse), bzw. mit eindeutig definierten und zugewiesenen Rechten und Rollen entsprechend den Anforderungen der DFN-AAI Verlässlichkeitsklasse 3 (siehe https://www.aai.dfn.de/der-dienst/verlaesslichkeitsklassen/).

g. Die Authentifizierung erfolgt mindestens mittels Passwort, wobei angemessene Vorgaben zur Sicherheit der Passwörter technisch implementiert sein müssen.

3. Datensicherung
    a. Datensicherungen erfolgen grundsätzlich täglich. In regelmäßigen Abständen werden Kopien an einem räumlich entfernten Ort hinterlegt; für diesen Ort gelten dieselben Anforderungen zum Schutz der Infrastruktur wie in 2. beschrieben.
    b. Es wird sichergestellt, dass Backups in angemessener Zeit in das produktive System eingespielt werden können. Hierzu finden mindestens einmal jährlich Tests statt.

4. Protokollierung
    a. Änderungen der personenbezogenen Daten in automatisierten Dateien gemäß § 3 Abs. 7 ThürDSG werden protokolliert. Dabei werden die An- und Abmeldung des Benutzers im System, die Änderung an sich, der Zeitpunkt der Änderung und der ändernde Benutzer erfasst.
    b. Die Benutzer sind spätestens mit der Rechtevergabe über die Protokollierung in Kenntnis zu setzen.
    c. Die Protokollierung ist nach angemessener Zeit zu löschen.

5. Personal
    a. Zugriff auf personenbezogene Daten wird regelmäßig nur Mitarbeitern der Vertragsparteien gewährt.
    b. Mitarbeiter sind, bevor ihnen der Zugriff auf personenbezogene Daten gewährt wird, über ihre Pflichten zur Beachtung des Datenschutzes im Allgemeinen zu belehren. Vor Einführung neuer Verfahren und vor wesentlichen Änderungen bestehender Verfahren hat zudem eine Einweisung zu erfolgen, die auch besondere datenschutzrechtliche Anforderungen des konkreten Verfahrens umfasst. Dazu gehören insbesondere Belehrungen über Protokollierungen, die Nutzung des Zugriffs auf personenbezogene Daten ausschließlich zu dienstlichen Zwecken und notwendige Sicherheitsvorkehrungen. Die Belehrungen sind zu dokumentieren.
    c. Fremdpersonal, das Zugang zu personenbezogenen Daten erlangen könnte, ist in dokumentierter Form einzuweisen und zu beaufsichtigen.
    d. Im Rahmen von Heimarbeit besteht kein Zugang zu personenbezogenen Daten. Eine Verarbeitung personenbezogener Daten findet in Heimarbeit nicht statt. Die Sätze 1 und 2 gelten nicht, soweit die Verarbeitung personenbezogener Daten in Heimarbeit nach den Regeln von Auftraggeberin und Auftragnehmerin zulässig ist und dies durch eine Freigabe durch die Datenschutzbeauftragten von Auftraggeberin und Auftragnehmerin dokumentiert ist.

6. Trennung verschiedener Auftraggeber
    a. Die Auftragnehmerin speichert und verarbeitet personenbezogene Daten verschiedener Auftraggeber grundsätzlich voneinander getrennt.
    b. Die Speicherung personenbezogener Daten, die von verschiedenen Auftraggebern zur Verfügung gestellt werden, in einer Datei ist unzulässig.
    c. Ausgenommen von dem Gebot der Trennung sind solche personenbezogenen Daten, die zur Auftragsabwicklung erforderlich sind, wie Name, E-Mail, Telefonnummer der Ansprechpartner.