Universität Leipzig

Ordnung zum Datenschutz an der Universität Leipzig

Vom 13. Juni 2019

1. Allgemeines

1.1 Grundlagen

Grundlagen dieser Ordnung sind u.a.:

- Das Sächsische Datenschutzdurchführungsgesetz (SächsDSDG) vom 26. April 2018.
- Die EU-Datenschutz-Grundverordnung (DS-GVO) vom 27. April 2016.

1.2 Zweck

Zweck dieser Ordnung ist, die datenschutzkonforme Verarbeitung personenbezogener Informationen und Daten einschließlich der Datensicherheit (im folgenden Datenschutz genannt) durch die verarbeitenden Stellen der Universität Leipzig gemäß dem Recht auf informationelle Selbstbestimmung zu gewährleisten. Die Ordnung enthält Regelungen, wie die gesetzlichen Anforderungen zum Datenschutz an der Universität Leipzig umgesetzt werden.

1.3 Geltungsbereich

Diese Ordnung bezieht sich auf die Verarbeitung von personenbezogenen Daten im Hochschulbereich der Universität Leipzig. Sie muss gleichfalls für die Kommunikation und den Datenaustausch mit Dritten beachtet werden. Bereits bestehende Anweisungen und Regelungen der Universität sowie getroffene Dienstvereinbarungen mit dem Personalrat behalten ihre uneingeschränkte Gültigkeit. Sollten diese im Widerspruch zu dieser Ordnung stehen, ist der/die Kanzler/in unverzüglich in Kenntnis zu setzen.

1.4 Begriffsbestimmungen

Die in dieser Ordnung verwendeten Rollen- und Funktionsbezeichnungen gelten für alle Geschlechter.

Für die Begriffsbestimmungen gelten die Definitionen der DS-GVO und des SächsDSDG in der jeweils gültigen Fassung. Im Sinne dieser gesetzlichen Bestimmungen sind die von der Universität angestrebten Datenschutzziele:

- Zweckbindung/Datenminimierung: Personenbezogene Daten werden nur für festgelegte, eindeutige und legitime Zwecke erhoben und dürfen grundsätzlich nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Die Daten müssen auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Die Erhebung der Daten muss dem Zweck entsprechend und angemessen sein.
- Verfügbarkeit: Die Hard- und Software einschließlich der Daten stehen dann zur Verfügung, wenn sie tatsächlich gebraucht werden. Ein hohes Maß an Verfügbarkeit wird gewährleistet durch das leistungsoptimale Erbringen von erwünschten IT-Dienstleistungen eines Systems in der dafür vorgesehenen Zeit.
- Integrität: Die Nutzer können sicher sein, dass die Daten richtig, d. h. inhaltlich korrekt und ebenso vollständig sind. Die jeweiligen Informationen werden dabei nur durch Befugte und gleichfalls nur in der dafür vorgesehen Weise be- und verarbeitet.
- Vertraulichkeit: Nur Berechtigte haben den für ihre Aufgabenerfüllung notwendigen Zugang zu Informationen; kein/e Unbefugte/r erhält Kenntnis von personenbezogenen Daten.
- Authentizität: Die Empfänger können zweifelsfrei sicher sein, dass eine Information tatsächlich von dem/der genannten Verfasser/in geschaffen und nicht durch Dritte gefälscht oder anderweitig verändert wurde.
- Verbindlichkeit/Revisionsfähigkeit: Die an einer Transaktion Beteiligten sind tatsächlich autorisiert und verfügen über keinerlei Mittel, ihre Beteiligung zu bestreiten. Über (programmseitige) Dokumentationen ist nachvollziehbar, wer zu welchem Zeitpunkt welche Änderungen vorgenommen hat.
- Transparenz: Die einzelnen Verfahrensschritte während der Datenverarbeitung sind vollständig, aktuell und werden so dokumentiert, dass sie in zumutbarer Zeit ebenfalls nachvollzogen werden können.

Diese Datenschutzziele werden an der Universität in sämtlichen technischen, organisatorischen und infrastrukturellen Bereichen angestrebt.

2. Zuständigkeitsregelungen

2.1 Grundsätze

Die grundsätzliche Datenschutzstrategie der Universität lässt sich wie folgt zusammenfassen:

- Der Datenschutz ist Verantwortung und zugleich integraler Bestandteil des Handelns des Rektorates.
- Die Universität schützt die von ihr zu verarbeitenden personenbezogenen Daten im Interesse aller ihrer Mitglieder und Angehörigen und wahrt die Rechte der von der Datenverarbeitung Betroffenen.
- Die Gewährleistung von Datenschutz und Datensicherheit sowie der Schutz von Ressourcen ist eine selbstverständliche Aufgabe und Pflicht im Rahmen eines rechtmäßigen und ordnungsgemäßen Handelns für alle Mitglieder und Angehörige der Universität.
- Die Prozesse der personenbezogenen Datenverarbeitung müssen für alle Beteiligten nachvollziehbar sein.
- Der Zugriff und die Verarbeitung von personenbezogenen Daten erfolgen ausschließlich in dem Umfang, wie es für die konkrete Aufgabenerfüllung erforderlich ist.

2.2 Zentrale Datenschutzfunktionen

Zur Wahrung des Datenschutzes richtet die Universität zwei zentrale Elemente ein. Neben dem/der unabhängigen Datenschutzbeauftragten wird die Universitätsleitung bei der Wahrnehmung ihrer Pflichten durch eine/n Datenschutzmanager/in unterstützt, den/die sie mit dem Aufbau und dem Betrieb eines Datenschutzmanagementsystems (DSMS) beauftragt und mit den erforderlichen Ressourcen ausstattet.
Das DSMS soll ein, auf ständige Leistungsverbesserung, systematische und klare Lenkung und Leitung ausgerichtetes Konzept sein, um die Universität in Bezug auf den Datenschutz erfolgreich führen und betreiben zu können.

2.2.1 Behördliche/r Datenschutzbeauftragte/r

<u>Stellung/Befugnisse</u>
Der/Die von der Universität bestellte behördliche Datenschutzbeauftragte ist in dieser Eigenschaft weisungsfrei, kann sich unmittelbar an das Rektorat wenden und darf wegen der Erfüllung seiner/ihrer Aufgaben nicht benachteiligt werden. Er/Sie wird vom Rektorat mit den für die Aufgabenerfüllung erforderlichen Ressourcen ausgestattet. Der/Die behördliche Datenschutzbeauftragte ist zur Wahrung der Geheimhaltung und Vertraulichkeit verpflichtet.

<u>Aufgaben</u>
Er/Sie:
- ist Ansprechpartner/in für alle von der Datenverarbeitung betroffenen Personen und berät diese in allen Fragen, die mit der

Verarbeitung ihrer personenbezogenen Daten und der Wahrnehmung ihrer Rechte gemäß DS-GVO zusammenhängen,
- unterrichtet und berät die Leitung der Universität und die Mitglieder und Angehörigen der Universität bei der Sicherstellung des Datenschutzes,
- überwacht die Einhaltung der DS-GVO und sonstiger datenschutzrechtlicher Vorschriften,
- ist über geplante Verfahren der automatisierten Verarbeitung personenbezogener Daten zu unterrichten, sensibilisiert und schult in Absprache mit dem/der Datenschutzmanager/in die an den Verarbeitungsvorgängen beteiligten Mitglieder und Angehörigen der Universität,
- berät die Verantwortlichen bei der Erstellung und Anpassung von Ordnungen, Richtlinien, Anweisungen und Dienstvereinbarungen mit datenschutzrechtlichem Bezug,
- berät auf Anfrage bei der Erstellung der Datenschutz-Folgenabschätzungen und überwacht deren Durchführung,
- arbeitet in Abstimmung mit dem/der Datenschutzmanager/in mit den Aufsichtsbehörden zusammen,
- trägt bei der Erfüllung der Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung, wobei er/sie die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigt.
- Alle Mitglieder und Angehörige der Universität sowie alle von der Datenverarbeitung betroffenen Personen können sich in Fragen des Datenschutzes unmittelbar an die/den behördliche/n Datenschutzbeauftragte/n wenden.

2.2.2 Datenschutzmanager/in

<u>Stellung / Befugnisse</u>

Der/Die vom Rektorat beauftragte Datenschutzmanager/in unterstützt die Universitätsleitung bei der Wahrnehmung ihrer Pflichten als Verantwortliche für den Datenschutz, der Einhaltung und Überprüfung der Regelungen dieser Ordnung sowie der einschlägigen gesetzlichen Bestimmungen zum Datenschutz. Er/Sie ist im Referat für Datenschutz und Informationssicherheit angesiedelt und berichtet in regelmäßigen Abständen sowie bei besonderen Vorkommnissen dem Rektorat unverzüglich. Er/Sie ergreift in Abstimmung mit den jeweiligen Verantwortlichen und den Verarbeitern die erforderlichen Maßnahmen, um die Erfüllung derer Pflichten zu gewährleisten.

Aufgaben

Der/Die Datenschutzmanager/in ist mit der Einführung und dem Betrieb eines Datenschutzmanagementsystems (DSMS) betraut. Er/Sie:

- arbeitet in datenschutzrechtlichen Angelegenheiten vertrauensvoll mit allen Stellen der Universität, insbesondere mit dem/der Datenschutzbeauftragten zusammen,
- berät die jeweils verfahrensverantwortlichen Stellen bei der Erstellung das Verzeichnis der Verarbeitungstätigkeiten (gem. Art. 30 DS-GVO) und führt eine Übersicht über alle Verzeichnisse im DSMS,
- koordiniert im Zusammenwirken mit den verfahrensverantwortlichen Stellen die systematische Erstellung von Prozessbeschreibungen von allen Abläufen bei denen personenbezogene Daten verarbeitet werden,
- führt im Auftrag der Verantwortlichen die Datenschutz-Folgeabschätzung (DSFA) durch und holt hierbei erforderlichenfalls den Rat des/der Datenschutzbeauftragten ein,
- ist durch die Verfahrensverantwortlichen bei der Planung und Einführung neuer Verfahren zur Verarbeitung von personenbezogenen Daten unverzüglich zu beteiligen; gleiches gilt für den beabsichtigten Abschluss von Verträgen zur Auftragsverarbeitung,
- übernimmt das systematische Management sämtlicher datenschutzrechtlich relevanter Dokumente, insbesondere der Verträge zur Auftragsdatenverarbeitung,
- führt, im Zusammenwirken mit dem/der Datenschutzbeauftragten, adressatengerechte Schulungen zu datenschutzrechtlichen Themen durch und konzipiert entsprechende Informationsangebote,
- ist, unbeschadet der Aufgabe des/der Datenschutzbeauftragten, Ansprechperson der Verfahrensverantwortlichen bei Anfragen zu Betroffenenrechten und nimmt in Abstimmung mit dem/der Kanzler/in die Pflichten zur Kommunikation mit den Aufsichtsbehörden (insbesondere Meldung von datenschutzrechtlichen Verstößen) wahr.

Ihm/Ihr obliegt überdies federführend die Überprüfung und falls erforderlich die Anpassung dieser Ordnung sowie des DSMS.

2.3 Verfahrensverantwortliche

Die Leitung der jeweiligen Einrichtung ist verantwortlich für die Organisation des Datenschutzes in ihrem Bereich. Sie kann je nach Erforderlichkeit einen oder mehrere Zuständige benennen, die bei der Umsetzung des Datenschutzes, ggf. in Abstimmung mit dem/der Verantwortlichen für Informations- und Kommunikationstechnik der Einrichtung, mitwirken. Weiterhin bestimmt die Leitung der Einrichtung Verfahrensverantwortliche für jeden Geschäftsprozess und jedes IT-Verfahren, in dem personenbezogene Daten verarbeitet werden. Die benannten Verfahrensverantwortlichen sind Ansprechperson für Mitglieder und Angehörige und arbeiten mit den unter 2.2 benannten Stellen zusammen.
Bei hochschulweit gleichartiger Verarbeitung personenbezogener Daten durch mehrere Stellen ist ein/e Verfahrensverantwortliche/r zu bestimmen. Diese/r soll die Anforderungen des Datenschutzes koordinieren und steuern. Er/Sie erlässt in Abstimmung mit dem/der Datenschutzmanager/in grundlegende Vorgaben zur Einhaltung des Datenschutzes für alle an der Verarbeitung beteiligten Stellen. Wird von diesen Vorgaben abgewichen, muss die Abweichung durch die verantwortliche Stelle im Verzeichnis der Verarbeitungstätigkeiten dokumentiert werden.

2.3.1 Verarbeitungstätigkeiten

Die Verfahrensverantwortlichen dokumentieren die Verarbeitung personenbezogener Daten in einem Verzeichnis der Verarbeitungstätigkeiten nach Anlage 1. Dieses Verzeichnis verbleibt bei der verarbeitenden Stelle. Nutzen mehrere Stellen gleichartige Verfahren, können gemeinsame Verzeichnisse erstellt werden. Dem/Der Datenschutzmanager/in ist eine Kopie zu übersenden. Die Verzeichnisse sind regelmäßig zu überprüfen und bei Änderungen der Verarbeitungstätigkeit oder seiner Rahmenbedingungen anzupassen. Nach Einführung eines DSMS erfolgt die Dokumentation der Verarbeitungstätigkeiten in diesem System.

2.3.2 Auftragsverarbeitung

Erfolgt die Verarbeitung von personenbezogenen Daten durch Dritte muss eine Vereinbarung zur Auftragsverarbeitung (Art. 28 DSG-VO) nach dem Muster in Anlage 2 mit dem Auftragnehmer geschlossen werden. Die Vereinbarungen sind nach der Prüfung durch den/die Datenschutzmanager/in durch den/die Kanzler/in zu unterschreiben.

2.3.3 Datenschutz-Folgeabschätzungen

Hat eine Verarbeitung voraussichtlich hohe Risiken für die persönlichen Rechte und Freiheiten der Betroffenen zur Folge, so muss der/die Verfahrensverantwortliche in Zusammenarbeit mit dem/der Datenschutzmanager/in eine Datenschutz-Folgeabschätzung (Art. 35 DS-GVO) durchführen. Dabei sind Eintrittswahrscheinlichkeit und Schwere der möglichen Risiken zu bewerten und Maßnahmen zur Eindämmung der Risiken festzulegen. Der/Die Verfahrensverantwortliche muss den/die Datenschutzbeauftragte/n beteiligen. Gegebenenfalls muss er den/die Sächsische/n Datenschutzbeauftragte/n konsultieren (Art. 36 DS-GVO).

2.3.4 Informationspflichten

Werden personenbezogene Daten bei Betroffenen direkt erhoben, muss der/die Verfahrensverantwortliche Informationen nach Art. 13 Abs. 1 und 2 DS-GVO erstellen und den Betroffenen Zugriff darauf gewähren.

3. Betroffenenrechte

Die Rechte von Betroffenen sind möglichst unverzüglich, spätestens jedoch nach gesetzlicher Frist (1 Monat, Verlängerung in begründeten Ausnahmefällen) zu erfüllen. Die anfragende Person ist zweifelsfrei zu identifizieren. Vor der Herausgabe, Veränderung oder Löschung von Daten ist zu prüfen, ob Rechte Dritter beeinträchtigt oder rechtmäßige Forschungsvorhaben dadurch unverhältnismäßig beeinträchtigt werden.

3.1 Auskunftsersuchen und Berichtigung

Persönliche Auskünfte und Berichtigungsersuchen zu verarbeiteten Daten sollten durch die verarbeitende Stelle möglichst pragmatisch gehandhabt werden. Nach Identifikation der Person sind Anfragen im Rahmen der Möglichkeiten und unter Wahrung der Verhältnismäßigkeit, der dienstlichen Aufgaben und der Rechte Dritter zu beantworten bzw. zu bearbeiten. Die Auskunft kann auch über den/die Datenschutzmanager/in erfolgen.
Auskunftsersuchen, die nicht unmittelbar durch die verarbeitende Stelle beantwortet werden können, weil beispielsweise mehrere Stellen die angefragten personenbezogenen Daten verarbeiten, werden durch den/die Datenschutzmanager/in beantwortet. Diese/r koordiniert die Abfrage bei allen betroffenen verarbeitenden Stellen.

Bei Auskunftsersuchen von Dritten ist zwingend die Rechtmäßigkeit/ Rechtsgrundlage der Auskunftserteilung und die Authentizität der anfragenden Stelle zu überprüfen. In Zweifelsfällen ist der/die Datenschutzbeauftragte hinzuzuziehen.
Die Änderung von personenbezogenen Daten erfolgt ausschließlich nach Nachweis der Richtigkeit der Änderungen.

3.2 Löschung und Widerspruch

Die Löschung von Daten soll regelmäßig nach Ablauf der Löschfristen erfolgen. Personenbezogene Daten nach Widerspruch zur Verarbeitung bzw. auf Verlangen der Betroffenen zu löschen ist nur zulässig, wenn die Daten nicht mehr zu dienstlichen Zwecken oder für Forschungsvorhaben benötigt werden und gesetzliche Aufbewahrungsfristen der Löschung nicht entgegenstehen. Gesetzliche Regelungen wie das sächsische Archivgesetz sind zu beachten.

4. Besondere Zuständigkeiten

4.1 Dezernat 3 – Bereich Personal

Das Dezernat 3 – Bereich Personal ist für folgende datenschutzrelevanten Aufgaben zuständig:

- Verpflichtung auf Vertraulichkeit bei der Begründung von Beschäftigungsverhältnissen aller Art. Ein entsprechendes Formular ist als Anlage 3 enthalten.
- Ergreifen von arbeits- oder disziplinarrechtlichen Maßnahmen aufgrund von Verstößen gegen die sich aus den Bestimmungen zum Datenschutz und anderen Schutz- und Geheimhaltungsvorschriften sowie der Verpflichtung auf Vertraulichkeit ergebenden Pflichten.
- Initiale Information der Beschäftigten zur Verarbeitung ihrer personenbezogenen Daten an der Universität zur Wahrung der Informationspflicht nach Art. 13 DS-GVO.

4.2 Forschung

Werden personenbezogene Daten im Rahmen der wissenschaftlichen Forschung verarbeitet, sind geeignete Maßnahmen zum Schutz dieser Daten zu treffen. Für Forschungsvorhaben ist das Verzeichnis der Verarbeitungstätigkeiten durch den/der Verantwortlichen des Forschungsvorhabens anzufertigen. Insbesondere im Sinne der Datenminimierung sind, soweit es das Ziel der Forschung nicht beeinträchtigt, die Daten zu pseudonymisieren oder bestenfalls zu anonymisieren. Auf die Regelungen zur

Verarbeitung personenbezogener Daten zu wissenschaftlichen oder historischen Forschungszwecken in § 12 SächsDSDG wird explizit verwiesen.

5. Meldepflichten

Werden Verstöße gegen die Datenschutzbestimmungen bekannt, sind diese unverzüglich durch die Verfahrensbetreiber abzustellen. Fehlerhafte Daten sind zu berichtigen. Sind durch diesen Verstoß möglicherweise die Rechte der Betroffenen beeinträchtigt, so ist diese Datenschutzverletzung sofort dem/der Datenschutzmanager/in zu melden. Diese/r benachrichtigt die betroffenen Personen. Zur Meldung von Datenschutzverletzungen/-verstößen kann auch der/die Datenschutzbeauftragte vertraulich kontaktiert werden. Können die Datenschutzverletzungen zu einem erheblichen Risiko für die Rechte und Freiheiten natürlicher Personen oder zu einer schwerwiegenden Beeinträchtigung für die Rechte oder schutzwürdigen Interessen der Betroffenen führen, entscheidet der/die Kanzler/in nach Konsultation des/der Datenschutzbeauftragten über eine Meldung (Art. 33 DS-GVO) an den/die Sächsische/n Datenschutzbeauftragte/n. Diese Meldung erfolgt spätestens 72 Stunden nach Bekanntwerden der Datenschutzverletzung.

6. Inkrafttreten

Diese Ordnung wurde am 4. April 2019 vom Rektorat und am 7. Mai 2019 vom Senat der Universität Leipzig beschlossen. Sie tritt am Tag nach ihrer Bekanntmachung in den Amtlichen Bekanntmachungen der Universität Leipzig in Kraft.

Leipzig, den 13. Juni 2019

Prof. Dr. med. Beate A. Schücking
Rektorin

Verzeichnis über die Verarbeitungstätigkeiten gemäß Art. 30 DSGVO

Verantwortlicher:

Name des Verfahrens: z.B. Personalverwaltung, Zeiterfassung etc.

Zweck der Datenverarbeitung

Bitte möglichst konkret angeben/beschreiben.

Beschreibung des Verfahren:

Bitte möglichst konkret angeben/beschreiben, ausführliche Beschreibung aller Datenflüsse, ggf. Abgrenzung von anderen Prozessen.

Zuständige/r Fachbereich/e:

☐ Gemeinsames Verfahren — Ggf. bitte andere Stelle und deren Leiter angeben!

Ausfüllender Mitarbeiter:

Funktion:
Name:
Tel. (dienstl.):
E-Mail (dienstl.):

Einführungstermin: TT.MM.JJJJ

Rechtsgrundlage der Datenverarbeitung

☐ Einwilligung gemäß Art. 6 Abs. 1 a DSGVO

☐ Vertrag gemäß Art. 6 Abs. 1 b DSGVO

☐ rechtliche Verpflichtung gemäß Art. 6 Abs. 1 c DSGVO

Bitte Norm angeben, ggf. Anmerkungen.

☐ lebenswichtige Interessen gemäß Art. 6 Abs. 1 d DSGVO

Bitte erläutern.

☐ öffentliche/s Interesse/Gewalt gemäß Art. 6 Abs. 1 e DSGVO

Bitte erläutern.

☐ Berechtigte Interessen gemäß Art. 6 Abs. 1 f DSGVO

Bitte erläutern und Interessenabwägung darlegen.

☐ Sonstige Erlaubnisgrundlage:

Bitte Norm angeben, ggf. Anmerkungen.

Kategorien der betroffenen Personen und der diesbezüglich verarbeiteten Daten:

☐ Beschäftigte

Bitte konkrete Angabe der Datenkategorien, z.B. Kontaktdaten, Bankverbindung, Sozialversicherungsdaten, Krankentage etc.

☐ Bewerber

Bitte konkrete Angabe der Datenkategorien, z.B. Kontaktdaten, Bankverbindung, Sozialversicherungsdaten, Krankentage etc.

☐ ehemalige Beschäftigte

Bitte konkrete Angabe der Datenkategorien, z.B. Kontaktdaten, Bankverbindung, Sozialversicherungsdaten, Krankentage etc.

☐ Kunden

Bitte konkrete Angabe der Datenkategorien, z.B. Kontaktdaten, Bankverbindung, Sozialversicherungsdaten, Krankentage etc.

☐ Lieferanten

Bitte konkrete Angabe der Datenkategorien, z.B. Kontaktdaten, Bankverbindung, Sozialversicherungsdaten, Krankentage etc.

☐ Sonstige: Bitte konkret angeben!

☐ Sonstige: Bitte konkret angeben!

☐ Sonstige: Bitte konkret angeben!

Besondere Kategorien:

☐ Rassische/ethnische Herkunft	Bitte konkret angeben
☐ Religiöse/weltanschauliche Überzeugnungen	Bitte konkret angeben
☐ Sexualleben/sexuelle Orientierung	Bitte konkret angeben
☐ Politische Meinungen	Bitte konkret angeben
☐ Gesundheit	Bitte konkret angeben
☐ Genetische Daten	Bitte konkret angeben
☐ Biometrische Daten	Bitte konkret angeben
☐ Gewerkschaftszugehörigkeit	Bitte konkret angeben

Herkunft der Daten:

Bitte konkret angeben, z.B. Befragung des Betroffenen, Schnittstelle zu bzw. Übernahme aus anderem Verfahren, Übermittlung durch Dritten etc.

Regelfristen für die Löschung der Daten:

☐ automatisch ☐ manuell — ggf. Anmerkungen

☐ fristabhängge Löschung - Dauer: — z.B. 1 Woche nach Erhebung

☐ anlassbezogene Löschung - Anlass: — z.B. Kündigung, Widerruf/Widerspruch

☐ Sonstige: Bitte konkret angeben!

Zugriffsberechtigte Personengruppen (Berechtigungsgruppen; Funktionsträger):

Zugriffsberechtigte	Zweck, Art, Umfang
z.B. Abteilung,Funktionsträger	z.B. Buchhaltung, nur lesend, nur auf

Kategorien der Empfängern (intern, extern, Dienstleister, auch Konzernmitglieder)

☐	Interner Empfänger (Abt., Fkt.träger etc.)	Zweck der Weitergabe (Datenkategorien)
☐	Interner Empfänger (Abt., Fkt.träger etc.)	Zweck der Weitergabe (Datenkategorien)
☐	Interner Empfänger (Abt., Fkt.träger etc.)	Zweck der Weitergabe (Datenkategorien)
☐	Vertrag mit Auftragsverarbeiter*	Zweck der Weitergabe (Datenkategorien)
☐	Wartung/Support*	Zweck der Weitergabe (Datenkategorien)
☐	Kooperationsvereinbarung*	Zweck der Weitergabe (Datenkategorien)
☐	Externer Empfänger (Dritter, Behörde)	Zweck der Weitergabe (Datenkategorien)
☐	Externer Empfänger (Dritter, Behörde)	Zweck der Weitergabe (Datenkategorien)
☐	Externer Empfänger (Dritter, Behörde)	Zweck der Weitergabe (Datenkategorien)
☐	Sonstiges	Zweck der Weitergabe (Datenkategorien)
☐	Sonstiges	Zweck der Weitergabe (Datenkategorien)

Übermittlung in Drittländer bzw. an internationale Organisation:

Land	Unternehmen
Zweck der Weitergabe (Datenkategorien)	
Angabe der geeigneten Garantien z.B. Angemessenheitsbeschluss der EU, Standardvertragsklauseln C/C bzw. C/P, Aufsichtsbehördlich genehmigter Vertrag, Binding Corporate Rules	

Land	Unternehmen
Zweck der Weitergabe (Datenkategorien)	
Angabe der geeigneten Garantien z.B. Angemessenheitsbeschluss der EU, Standardvertragsklauseln C/C bzw. C/P, Aufsichtsbehördlich genehmigter Vertrag, Binding Corporate Rules	

Land	Unternehmen
Zweck der Weitergabe (Datenkategorien)	
Angabe der geeigneten Garantien z.B. Angemessenheitsbeschluss der EU, Standardvertragsklauseln C/C bzw. C/P, Aufsichtsbehördlich genehmigter Vertrag, Binding Corporate Rules	

Technische Angaben:

Zuständige/r Mitarbeiter der IT:

Funktion: Name: Tel. (dienstl.): E-Mail (dienstl.):	Funktion: Name: Tel. (dienstl.): E-Mail (dienstl.):

☐ Eigenentwickelte Software ☐ Standard- bzw. Kauf-Software

☐ Softwarebeschreibung

ggf. Anmerkungen

Lokale Anwendung:

☐ PC ☐ Laptop ☐ Sonstiges ☐ Sonstiges

ggf. Anmerkungen, z.B. private Endgeräte

Zentrale Anwendung:

☐ Client-/Serveranwendung ☐ Sonstiges ☐ Sonstiges

ggf. Anmerkungen

Netzanbindung:

☐ öffentlich, z.B. Internet, WLAN oder andere drahtlose Netzwerke ☐ intern

ggf. Anmerkungen

Anonymisierung/Pseudonymisierung:

☐ Anonymisierung ☐ Pseudonymisierung

☐ Alle Daten ☐ Folgende Daten

ggf. Anmerkungen, z.B. Zeitpunkt innerhalb des Verfahrens

Berechtigungsvergabe:

Durch wen erfolgt die Berechtigungsvergabe technisch/inhaltlich?
Wie erfolgt die Berechtigungsvergabe, z.B. über zentrales ADS, innerhalb der Anwendung?
Ggf. sonstige Anmerkungen

Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen:

Bitte möglichst konkret beschreiben!

☐ vgl. Folgenabschätzung bzw. sonstige Dokumentationen

☐ Information der Betroffenen gem. Art. 13 bzw. 14 DSGVO

☐ vgl. Vertrag zur Auftragsverarbeitung (Anlage TOMs)

☐ vgl. Datenschutz-Zertifizierung

☐ vgl. IT-Sicherheitskonzept

Bitte Abweichungen bzw. Ergänzungen konkret angeben!

UNIVERSITÄT LEIPZIG

Vertrag zur Auftragsverarbeitung nach Art. 28 Abs. 3 DS-GVO[1]

Zwischen der
hier eintragen
– nachstehend Auftraggeber (Verantwortlicher) genannt –
und der xyz
– nachstehend Auftragnehmer (Auftragsverarbeiter) genannt –

wird folgende Vereinbarung getroffen:

1. Gegenstand und Dauer der Vereinbarung

Der Auftrag umfasst Folgendes:

(Gegenstand des Auftrags, konkrete Beschreibung der Dienstleistungen / Anlage möglich)

Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage dieses Vertrages.

Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

[1] EU-Datenschutzgrundverordnung (DS-GVO) - VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

Dauer des Auftrags

Der Vertrag beginnt am
und endet am
oder
wird auf unbestimmte Zeit geschlossen.
Kündigungsfrist ist

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

2. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen:

nähere Beschreibung, ggf. Verweis auf Leistungsverzeichnis als Anlage etc.

Art der Verarbeitung (entsprechend der Definition von Art. 4 Nr. 2 DS-GVO):
wie sollen die Daten verarbeitet werden? / Anlage möglich

Art der personenbezogenen Daten (entsprechend der Definition von Art. 4 Nr. 1, 13, 14 und 15 DS- GVO):
welche Daten sollen verarbeitet werden? / Anlage möglich

Kategorien betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DS-GVO):
welche Personen sind betroffen? / Bsp.: Probanden des Forschungsprojektes XYZ

3. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüg-

lich an diesen weiterzuleiten.

Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

Der Auftraggeber ist berechtigt, sich wie unter Nr. 5 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen
technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

4. Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragnehmers

Weisungsberechtigte Personen des Auftraggebers sind:
(Bitte eintragen / (Vorname, Name, Organisationseinheit, Telefon)

Weisungsempfänger beim Auftragnehmer sind:
(Bitte eintragen / (Vorname, Name, Organisationseinheit, Telefon)

Für Weisung zu nutzende Kommunikationskanäle:
(Bitte eintragen genaue postalische Adresse/ E-Mail/ Telefonnummer)

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

5. Pflichten des Auftragnehmers

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragnehmer dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DS-GVO).

Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt.

Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.

Der Auftragnehmer hat über die gesamte Abwicklung der Dienstleistung für den Auftraggeber zu Vertragsbeginn, und fortlaufend aller 2 Jahre, eine IS-Kurzrevision gemäß dem Leitfaden des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in der aktuellen Fassung in seinem Bereich durchzuführen. Das Ergebnis Kurzrevision ist zu dokumentieren und dem Auftraggeber unverzüglich zu übermitteln.

Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. e und f DS-GVO). Er hat die dazu erforderlichen Angaben jeweils unverzüglich an das Referat Datenschutz und Informationssicherheit weiterzuleiten.

Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach

gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DS-GVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.

Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.

Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DS-GVO).

Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt. Hierzu wird bis auf weiteres vereinbart, dass sich der Auftragnehmer sich damit einverstanden erklärt, dass sowohl der Auftraggeber als auch die für den Auftraggeber zuständige Aufsichtsbehörde für den Datenschutz 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. Der Auftraggeber ist nach angemessener Vorankündigung berechtigt dazu die Diensträume des Auftragnehmers zu den üblichen Geschäftszeiten zu betreten.

Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten des Auftragnehmers) ist nur mit Zustimmung des Auftraggebers gestattet. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist vorher der Zugang zur Wohnung des Beschäftigten für Kontrollzwecke des Arbeitgebers vertraglich sicher zu stellen. Die Maßnahmen nach Art. 32 DS-GVO sind auch in diesem Fall sicherzustellen.

Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutz- rechtlichen Vorschriften der DS-GVO bekannt sind.

Er verpflichtet sich, auch folgende für diesen Auftrag relevanten Geheimnisschutzregeln zu beachten, die dem Auftraggeber obliegen.

Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DS- GVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb**.**

Beim Auftragnehmer ist als Beauftragte(r) für den Datenschutz Herr/Frau
(Vorname, Name, Organisationseinheit, Telefon)
bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

Der Auftragnehmer verpflichtet sich, den Auftraggeber über den Ausschluss von genehmigten Verhaltensregeln nach Art. 41 Abs. 4 DS-GVO und den Widerruf einer Zertifizierung nach Art. 42 Abs. 7 DS-GVO unverzüglich zu informieren.

6. Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DS-GVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DS-GVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DS-GVO). Meldungen nach Art. 33 oder 34 DS-GVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

7. Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DS-GVO)

(Hinweis: Hier sind verschiedene Regelungsalternativen möglich. Die Parteien können ein absolutes Unterauftragsverbot vereinbaren, es kann aber auch ein Verbot mit Genehmigungsvorbehalt im Einzelfall geregelt werden. Auf letztere Möglichkeit bezieht sich der untenstehende Formulierungsvorschlag.)

Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit Genehmigung des Auftraggebers gestattet, Art. 28 Abs. 2 DS-GVO, welche auf einem der o. g. Kommunikationswege (Ziff. 4) mit Ausnahme der mündlichen Gestattung erfolgen muss. Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt. Außerdem muss der Auftragnehmer dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DS-GVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DS-GVO).

Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn

der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DS-GVO bezüglich seiner Beschäftigten erfüllt hat.

Der Auftragnehmer hat die Einhaltung der Pflichten des/der Subunternehmer(s) durch eine IS-Kurzrevision, im gleichen Turnus wie für den Auftragnehmer maßgeblich, gemäß dem Leitfaden des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in der aktuellen Fassung zu prüfen. Das Ergebnis der Kontrollen ist zu dokumentieren. Das Ergebnis der Überprüfungen ist dem Auftraggeber auf Verlangen zugänglich zu machen.

Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

Zurzeit sind für den Auftragnehmer die in Anlage *[bitte ergänzen]* mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.

Der Auftragnehmer informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DS-GVO).

(Hier haben die Vertragsparteien einen Gestaltungsspielraum: Entweder werden dem Auftragnehmer allgemein Befugnisse eingeräumt, Subunternehmer zu beauftragen oder dies wird von einer Einzelgenehmigung abhängig gemacht. Einigt man sich auf eine allgemeine Befugnis des Auftragnehmers zur Beauftragung von Subunternehmern, ist jede Subbeauftragung vorher durch den Auftragnehmer dem Auftraggeber anzuzeigen. Der Auftraggeber hat dann von Gesetzeswegen ein Recht auf Einspruch gegen diese Änderung (Art. 28 Abs. 2). Das Recht des Auftraggebers zum Einspruch ist im Vertrag ausdrücklich zu erwähnen. Da das Gesetz die Folgen dieses Einspruchs nicht regelt, wird empfohlen, hierzu vertragliche Regelungen zu finden. Wird keine Regelung getroffen, ist die Bestellung des Unterauftragnehmers, gegen den Einspruch erhoben wurde, nicht möglich.)

8. Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO (Art. 28 Abs. 3 Satz 2 lit. c DS-GVO)

Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DS-GVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

Für die auftragsgemäße Verarbeitung personenbezogener Daten erfolgt die Risikobewertung nach in Anlehnung an den BSI-Standard 100-3, welche die Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten berücksichtigt.

Das im Anhang *[nennen und beifügen]* beschriebene Datenschutzkonzept stellt die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragnehmer dar. Hierfür sind die Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in der jeweils aktuellen Fassung maßgeblich.

Eine regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der datenschutzkonformen Verarbeitung wird als verbindlich festgelegt. Hierfür ist der Leitfaden des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur IS-Kurzrevision in der aktuellen Fassung maßgeblich. Eine regelmäßige Überprüfung kann entfallen, wenn der Auftragnehmer für den Zeitraum und dem gesamten Umfang des Auftrages eine Zertifizierung nach ISO 27001 vorlegen kann.

Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragnehmer und Auftraggeber abzustimmen.

Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.

Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst

werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

9. Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DS-GVO

Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen.

oder
wie folgt datenschutzgerecht zu löschen bzw. zu vernichten/vernichten zu lassen:

Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

10. Vergütung

Optional / Kann auch im zugh. EVB-IT Vertrag geregelt werden

11. Haftung

Auf Art. 82 DS-GVO wird verwiesen.

Im Übrigen wird folgendes vereinbart:
Optional / Kann auch im zugh. EVB-IT Vertrag geregelt werden

12. Vertragsstrafe

Bei Verstoß des Auftragnehmers gegen die Regelungen dieses Vertrages, insbesondere zur Einhaltung des Datenschutzes, wird eine Vertragsstrafe von *[Bitte eintragen]* Euro vereinbart.
OPTIONAL / Kann auch im zugh. EVB-IT Vertrag geregelt werden / oder entfallen

13. Sonstiges

Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.
Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten 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.

Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Ort, Datum, Unterschrift	Ort, Datum, Unterschrift
Auftraggeber	Auftragnehmer

Dienststelle, in der die/der Beschäftigte tätig ist

_____

Name, Vorname der/des Beschäftigten Personalnummer

_____ _____

Verpflichtung
zur Einhaltung der datenschutzrechtlichen Anforderungen
nach der EU- Datenschutz-Grundverordnung

Mir ist bekannt, dass das Verarbeiten personenbezogener Daten grundsätzlich den Regelungen der EU-Datenschutz-Grundverordnung (DS-GVO), des Sächsischen Hochschulfreiheitsgesetzes (SächsHSFG) und des Datenschutzdurchführungsgesetzes (SächsDSDG) unterliegt.

Ein Merkblatt zu Begriffsbestimmungen in der DS-GVO, wichtigen Regelungen, an die ich mich bei meiner Tätigkeit besonders zu halten habe und zu Haftung und Sanktionen bei bestimmten Verstößen ist mir ausgehändigt worden. Ich bin darauf hingewiesen worden, dass die o. g. Rechtsvorschriften im Intranet auf der Homepage des Dezernates Finanzen und Personal unter: „Rechtliche Regelungen“ veröffentlicht sind und die DS-GVO und das SächsDSDG als Auslagen im Sekretariat des Dezernates Finanzen und Personal (Personalbereich) eingesehen werden können. Weitere Informationen zu datenschutzrechtlichen Fragestellungen erhalte ich bei Bedarf vom Datenschutzbeauftragten der Universität Leipzig (Tel.: 30081, E-Mail: dsb@uni-leipzig.de).

Ich verpflichte mich,

- **gemäß Art. 29 DS-GVO personenbezogene Daten ausschließlich auf Weisung des Verantwortlichen* zu verarbeiten, es sei denn, dass eine gesetzliche Verpflichtung zur Verarbeitung dieser Daten besteht und**
- **bei der Verarbeitung personenbezogener Daten die einschlägigen datenschutzrechtlichen Vorschriften einzuhalten, insbesondere die in Art. 5 DS-GVO geregelten Datenschutzgrundsätze.**

Mir ist bekannt, dass diese Verpflichtung nicht nur für das jetzige Arbeitsverhältnis gilt, sondern ebenso bei bloßen Vertragsverlängerungen im unmittelbaren Anschluss an das bisherige Arbeitsverhältnis und nach der Beendigung meiner Tätigkeit.

Mir ist bewusst, dass Verstöße gegen diese Verpflichtung/en

- mit Geldbuße, Geldstrafe und /oder Freiheitsstrafe geahndet werden,
- eine Verletzung von arbeitsvertraglichen Pflichten darstellen und
- Schadensersatzansprüche auslösen

können.

Leipzig, den _____ _____
Unterschrift der/des Beschäftigten

_____
Unterschrift der/des Verpflichtenden

* Verantwortlicher im Sinne der DS-GVO ist die Universität Leipzig; Als Weisung des Verantwortlichen gelten neben Einzelanweisungen der Vorgesetzten u. a. Verordnungen, Dienstvereinbarungen, allgemeine Dienstanweisungen, Prozessbeschreibungen, Ablaufpläne, betriebliche Dokumentationen und Handbücher.

Verteiler

Blatt 1 Personalakte
Blatt 2 Beschäftigte/r