UNIVERSITÄT
LEIPZIG

# Ordnung zum Datenschutz
## an der Universität Leipzig

1. Allgemeines

1.1 Grundlagen

1.2 Zweck

1.3 Geltungsbereich

1.4 Begriffsbestimmungen

2. Zuständigkeitsregelungen

2.1 Grundsätze

2.2 Zentrale Datenschutzfunktionen

2.2.1 Behördlicher Datenschutzbeauftragter

2.2.2 Datenschutzmanager

2.3 Verfahrensverantwortliche

2.3.1 Verarbeitungstätigkeiten

2.3.2 Auftragsverarbeitung

2.3.3 Datenschutz-Folgeabschätzungen

2.3.4 Informationspflichten

3. Betroffenenrechte

3.1 Auskunftsersuchen und Berichtigung

3.2 Löschung und Widerspruch

4. Besondere Zuständigkeiten

4.1 Dezernat 3 – Bereich Personal

4.2 Forschung

5. Meldepflichten

6. Inkrafttreten

# 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 die Kanzlerin 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 Unbefugter erhält Kenntnis von personenbezogenen Daten.
- **Authentizität:** Die Empfänger können zweifelsfrei sicher sein, dass eine Information tatsächlich von dem genannten Verfasser 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

#### Stellung / Befugnisse

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.

### Aufgaben

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 Datenschutzmanager 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 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 den behördlichen Datenschutzbeauftragten wenden.

## 2.2.2 Datenschutzmanager/in

### Stellung / Befugnisse

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 der Kanzlerin 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 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 die Kanzlerin 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 Sächsischen Datenschutzbeauftragten 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 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 in 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 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 die Kanzlerin nach Konsultation des/der Datenschutzbeauftragten über eine Meldung (Art. 33 DS-GVO) an den Sächsischen Datenschutzbeauftragten. 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.

Anlagen:
Anlage 1 – Muster Verzeichnis der Verarbeitungstätigkeiten
Anlage 2 – Muster Vereinbarung zur Auftragsdatenvereinbarung
Anlage 3 – Verpflichtung auf Vertraulichkeit