Datenschutz-Leitlinie der Carl von Ossietzky Universität Oldenburg

vom 28.08.2018

Das Präsidium der Carl von Ossietzky Universität Oldenburg hat am 29.05.2018 gemäß § 37 Abs. 1 S. 3 NHG in Verbindung mit Art. 4 Nr. 7 und 24 Abs. 1 der Europäischen Datenschutzgrundverordnung (EU-DSGVO) die nachfolgende Datenschutz-Leitlinie nach positiver Stellungnahme des behördlichen Datenschutzbeauftragten der Universität beschlossen.

Inhaltsverzeichnis

I. Präambel

Kernaufgabe des Datenschutzes ist es, das Recht einer jeden Person zu gewährleisten selbst über die Preisgabe und Verwendung ihrer Daten zu bestimmen (Recht auf informationelle Selbstbestimmung).

Die Verarbeitung von personenbezogenen Daten ist für das Funktionieren einer modernen Universität unerlässlich und hat nach den gesetzlichen Vorgaben u.a. der Europäischen Datenschutzgrundverordnung (EU-DSGVO) und dem Landesdatenschutzgesetz Niedersachsen (NDSG) zu erfolgen.

Das Umfeld der personenbezogenen Datenverarbeitung unterliegt hierbei, bedingt durch neue Techniken und Medien sowie der kontinuierlichen Anpassung von Geschäftsprozessen, einer permanenten Entwicklung.

Die Carl von Ossietzky Universität Oldenburg (Universität) ist sich ihrer gesetzlichen Aufgabe und der damit einhergehenden Verantwortung bewusst und macht in dieser Leitlinie ihre Datenschutzziele und die zur Erreichung dieser festgelegten Strategie und Aufgabenverteilung transparent.

Unabhängig von den gesetzlichen Vorgaben werden in einer gesonderten Leitlinie für Informationssicherheit die Sicherheitsziele und die Sicherheitsstrategie für die Umsetzung technischer und organisatorischer Maßnahmen festgelegt.

II. Geltungsbereich

Diese Leitlinie bezieht sich auf die Verarbeitung von personenbezogenen Daten an der gesamten Universität und ist verbindlich für alle Organisationseinheiten in Verwaltung und Wissenschaft und darüber hinaus verpflichtend für alle Mitglieder und Angehörige sowie Gäste der Universität.

Sie besitzt gleichfalls bindende Wirkung für die Kommunikation und den Datenaustausch mit Dritten.
Bereits bestehende Anweisungen und Regelungen der Universität sowie getroffene Dienstvereinbarungen mit dem Personalrat behalten ihre uneingeschränkte Gültigkeit. Sollten diese im Widerspruch zu dieser Leitlinie stehen ist die/der Referent/in für das Datenschutzmanagement unverzüglich in Kenntnis zu setzen.

III. Verantwortung

Die Verantwortung für die Einhaltung der gesetzlichen Bestimmungen zum Datenschutz und den Regelungen dieser Leitlinie liegt beim Präsidium der Universität.

In Erfüllung der gesetzlichen Vorgaben bestellt das Präsidium eine/n behördliche/n Datenschutzbeauftragte/n und stattet diese/n mit den für seine Aufgabenerfüllung erforderlichen Ressourcen aus.

Zur Wahrnehmung seiner eigenen Verantwortung sowie als Ausdruck des Bekenntnisses zum Datenschutz als Managementaufgabe benennt das Präsidium darüber hinaus eine/n Referentin/Referenten für das Datenschutzmanagement und beauftragt diese/n mit dem Aufbau und der Pflege eines Datenschutzmanagementsystems (DSMS).

Die Einhaltung der datenschutzrechtlichen Bestimmungen ist überdies Verpflichtung und Verantwortung aller Mitglieder und Angehörigen der Universität; deren Überwachung ist zugleich Aufgabe der Führungskräfte für ihren jeweiligen Bereich.

IV. Leitaussagen

Die grundsätzliche Datenschutzpolitik der Universität lässt sich in den folgenden fünf Leitaussagen zusammenfassen:

- Der Datenschutz ist Verantwortung und zugleich integraler Bestandteil des Handelns der Universitätsleitung.

- 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 erfolgt ausschließlich in dem Umfang, wie es für die konkrete Aufgabenerfüllung erforderlich ist.

V. Datenschutzziele

Im Sinne der gesetzlichen Bestimmungen sind die von der Universität angestrebten Datenschutzziele grundsätzlich auf die

- Zweckbindung/Datenminimierung
- Verfügbarkeit
- Integrität
- Vertraulichkeit
- Authentizität
- Verbindlichkeit und
- Transparenz

der zu verarbeitenden Daten ausgerichtet.

Im Rahmen des Sicherheitskonzeptes der Universität werden diese Datenschutzziele in sämtlichen technischen, organisatorischen sowie infrastrukturellen Bereichen angestrebt. Die vorgenannten Begriffe werden nachstehend wie folgt definiert:

- **Zweckbindung/Datenminimierung:** Personenbezogene Daten werden nur für festgelegte, eindeutige und legitime Zwecke erhoben und dürfen grundsätzlich nicht in einer mit diesen Zwecken nicht vereinbarenden Weise weiterverarbeitet werden. Sie müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.

- **Verfügbarkeit:** Ein hohes Maß an Verfügbarkeit wird gewährleistet durch das leistungsoptimale Erbringen von erwünschten IT-Dienstleistungen eines Systems in der dafür vorgesehenen Zeit. Die Hard- und Software einschließlich der Daten stehen dann zur Verfügung, wenn sie tatsächlich gebraucht werden.

- **Integrität:** Die Nutzerinnen/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 innerhalb ihrer Aufgabenerfüllung den Zugang zu den Informationen; kein Unbefugter erhält irgendwelche Kenntnisse.

- **Authentizität:** Die Empfängerin/der Empfänger kann 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 entsprechende (programmseitige) Dokumentationen ist es 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.

VI. Datenschutzstrategie

In Erfüllung der gesetzlichen Bestimmungen sowie als Ausprägung der eigenen Verantwortlichkeit setzt die Universität auf eine zweigleisige Strategie zur Erreichung der Datenschutzziele und Wahrung des Datenschutzes insgesamt.

Neben der gesetzlichen Verpflichtung zur Bestellung einer/eines unabhängigen, weisungsfreien behördlichen Datenschutzbeauftragten wird das Präsidium bei der Wahrnehmung seiner Pflichten insbesondere durch einen hierfür zu benennende/n Referentin/Referenten für das Datenschutzmanagement unterstützt, die/den es mit dem Aufbau und dem Betrieb eines Datenschutzmanagementsystems (DSMS) beauftragt und mit den hierfür erforderlichen Ressourcen ausstattet.

Das Präsidium setzt mit dem DSMS auf ein auf ständige Leistungsverbesserung, systematische und klare Lenkung und Leitung ausgerichtetes Konzept, um die Universität in Bezug auf den Datenschutz erfolgreich führen und betreiben zu können.

Ausgehend von dieser Leitlinie erlässt das Präsidium weitergehende spezifische Regelungen um den Schutz von personenbezogenen Daten in der Universität sicherzustellen.

1. Strategische Leitaussagen

Die Datenschutzstrategie der Universität lässt sich in den folgenden strategischen Leitaussagen zusammenfassen:

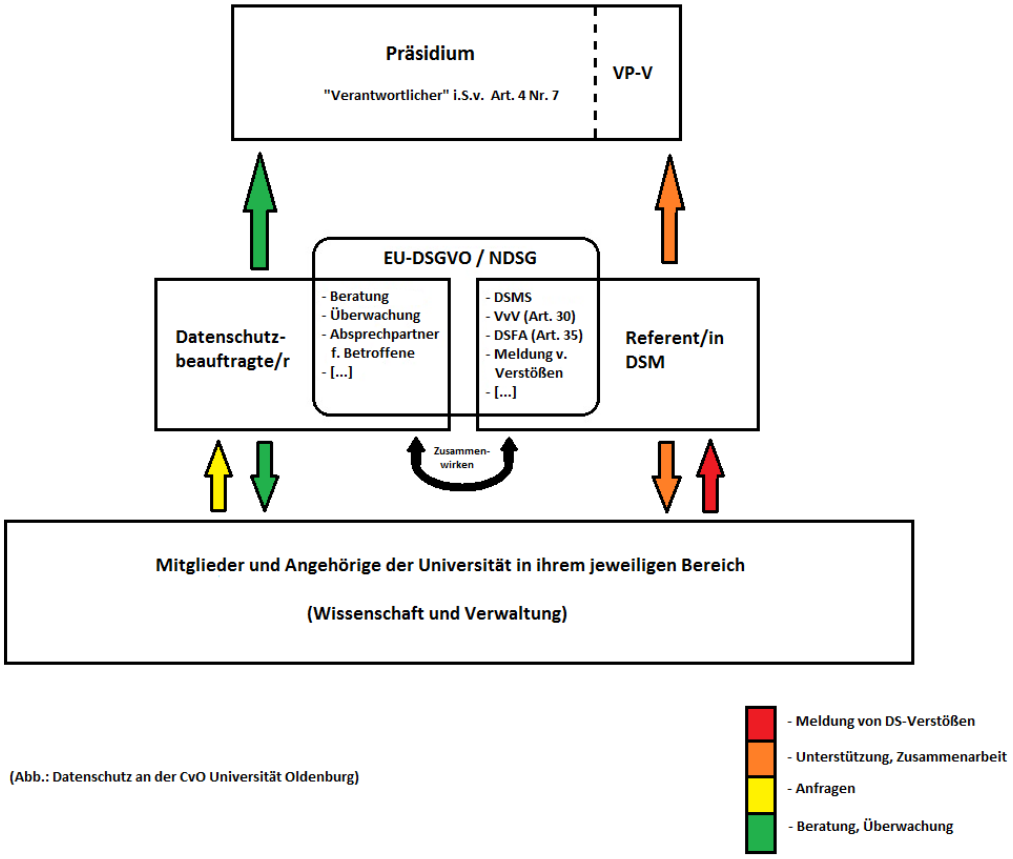
- Aufbau und Betrieb eines systematischen DSMS
- Schärfen des Bewusstseins für den Datenschutz durch entsprechende Informationen und Schulungen
- Sicherstellung der Erfüllung der gesetzlichen Bestimmungen und sich hieraus ergebenen Pflichten
- Transparente und eindeutige Verteilung von Aufgaben und Verantwortlichkeiten
- Überprüfung und Anpassung der getroffenen Maßnahmen

2. Organisatorischer Aufbau / Aufgaben

Wesentliche Akteure der Datenschutzstrategie der Universität sind

a. die/der behördliche Datenschutzbeauftragte
b. die/der Referent/in für das Datenschutzmanagement
c. alle Mitglieder und Angehörige der Universität (insb. Beschäftigte in Verwaltung und Wissenschaft).

Die Stellung, die Befugnisse und Aufgaben ergeben sich zum einen aus den einschlägigen gesetzlichen Bestimmungen und sind zum anderen Ausprägung des besonderen Bekenntnisses zum Datenschutz sowie des verfolgten systematischen Ansatzes zu dessen Sicherstellung.



(Abb.: Datenschutz an der CvO Universität Oldenburg)

a. Behördliche/r Datenschutzbeauftragte/r

Stellung / Befugnisse: Die/der vom Präsidium der Universität bestellte behördliche Datenschutzbeauftragte ist in dieser Eigenschaft weisungsfrei, kann sich unmittelbar an das Präsidium wenden und darf wegen der Erfüllung ihrer/seiner Aufgaben nicht benachteiligt werden. Er wird vom Präsidium mit den für seine Aufgabenerfüllung erforderlichen Ressourcen ausgestattet. Bei der Erfüllung seiner Aufgaben ist der behördliche Datenschutzbeauftragte zur Wahrung der Geheimhaltung und Vertraulichkeit verpflichtet.

Aufgaben: Sie/Er

- 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 DSGVO zusammenhängen,

- unterrichtet und berät die Leitung der Universität und die Beschäftigten bei der Sicherstellung des Datenschutzes

- überwacht die Einhaltung der DSGVO und sonstiger datenschutzrechtlicher Vorschriften,

- ist über geplante Verfahren der automatisierten Verarbeitung personenbezogener Daten zu unterrichten, sensibilisiert und schult (in Absprache mit der Referentin / dem Referenten für Datenschutzmanagement) die an den Verarbeitungsvorgängen beteiligten Mitarbeiter,

- berät – auf Anfrage – bei der Erstellung der Datenschutz-Folgenabschätzungen und überwacht deren Durchführung,

- arbeitet (in Abstimmung mit der Referentin / dem Referenten für Datenschutzmanagement) mit den Aufsichtsbehörden zusammen,

- trägt bei der Erfüllung seiner 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 die/den behördliche/n Datenschutzbeauftragte/n wenden.

b. Referent/in für das Datenschutzmanagement

Stellung / Befugnisse: Die/der vom Präsidium beauftragte Referent/in für das Datenschutzmanagement unterstützt die Universitätsleitung bei der Wahrnehmung ihrer Pflichten als Verantwortliche für den Datenschutz, der Einhaltung und Überprüfung der Regelungen dieser Leitlinie sowie der einschlägigen gesetzlichen Bestimmungen zum Datenschutz. Sie/er ist mit den für die Aufgabenerfüllung erforderlichen Ressourcen auszustatten, ist der/dem Vizepräsidentin/Vizepräsidenten für Verwaltung und Finanzen direkt unterstellt und berichtet diesem in regelmäßigen Abständen sowie bei besonderen Vorkommnissen unverzüglich. In Abstimmung mit diesem ergreift sie/er die erforderlichen Maßnahmen, um die Erfüllung der Pflichten des Verantwortlichen zu gewährleisten.

Aufgaben: Die/der Referent/in für das Datenschutzmanagement ist mit der Einführung und dem Betrieb eines Datenschutzmanagementsystems (DSMS) betraut.

Sie/er

- arbeitet in datenschutzrechtlichen Angelegenheiten vertrauensvoll mit allen Stellen der Universität, insbesondere mit der/dem Datenschutzbeauftragten zusammen,

- berät die jeweils verfahrensverantwortlichen Stellen bei der Erstellung der Verfahrensbeschreibungen und führt das Verzeichnis von Verarbeitungstätigkeiten (VvV, gem. Art. 30 DSGVO) für die Verantwortliche,

- führt im Auftrag des Verantwortlichen die Datenschutz-Folgeabschätzung (DSFA) durch und holt hierbei erforderlichenfalls den Rat der/des Datenschutzbeauftragten ein,

- ist bei der Planung und Einführung neuer Verfahren zur Verarbeitung von personenbezogenen Daten unverzüglich zu beteiligen; gleiches gilt für den beabsichtigten Abschluss von Verträgen zur Auftragsdatenverarbeitung,

- berät die Verantwortliche bei der Erstellung und Anpassung von Ordnungen, Richtlinien, Anweisungen und Dienstvereinbarungen mit datenschutzrechtlichem Bezug und wirkt an der Erstellung dieser mit,

- übernimmt das systematische Management sämtlicher datenschutzrechtlich relevanter Dokumente, insbesondere der Verträge zur Auftragsdatenverarbeitung,

- führt, im Zusammenwirken mit der/dem Datenschutzbeauftragten, adressatengerechte Schulungen zu datenschutzrechtlichen Themen durch und konzipiert entsprechende Informationsangebote,

- ist, unbeschadet der Aufgabe der/des Datenschutzbeauftragten, Ansprechpartner/in des Verantwortlichen bei Anfragen zu Betroffenenrechten und nimmt in Abstimmung mit der/dem Vizepräsidentin/Vizepräsidenten für Verwaltung und Finanzen die Pflichten des Verantwortlichen zur Kommunikation mit den Aufsichtsbehörden (insbesondere Meldung von datenschutzrechtlichen Verstößen) wahr.

Ihr/ihm obliegt überdies federführend die Überprüfung und erforderlichenfalls Anpassung dieser Leitlinie sowie des DSMS als solches.

c. Mitglieder und Angehörige der Universität

Alle Mitglieder und Angehörige der Universität sind zur Einhaltung der Regelungen dieser Leitlinie sowie der einschlägigen gesetzlichen Bestimmungen in ihrem Arbeitsbereich ebenso verpflichtet wie zur unverzüglichen Meldung von datenschutzrechtlichen Verstößen und Problemen an die/den Referentin/Referenten für das Datenschutzmanagement.

Jede Führungskraft ist namentlich Verfahrensverantwortliche/r in ihrem/seinem Aufgabenbereich. Dies umfasst die Verantwortung für die ordnungsgemäße Aufgabenerfüllung sowie den sorgsamen Umgang mit personenbezogenen Daten unabhängig, ob es sich um ein manuelles, technisches oder IT-gestütztes Verfahren handelt. Sie wirken auf die Einhaltung der Pflichten in ihrem Verantwortungsbereich hin und motivieren ihre Mitarbeiterinnen und Mitarbeiter für die Zielsetzungen dieser Leitlinie sowie die Wichtigkeit des Datenschutzes insgesamt. Sie werden hierbei – auf Anfrage – von der/dem Referentin/Referenten für das Datenschutzmanagement sowie der/dem Datenschutzbeauftragten unterstützt.

3. Technisch- und organisatorische Maßnahmen

Die Universität trifft diejenigen technischen und organisatorischen Maßnahmen, die erforderlich sind, um eine den gesetzlichen Bestimmungen entsprechende Verarbeitung personenbezogener Daten sicherzustellen. Der Aufwand für die Maßnahmen muss unter Berücksichtigung des Standes der Technik in einem angemessenen Verhältnis zu dem angestrebten Zweck stehen.
Soweit die Universität personenbezogene Daten verarbeitet, trifft sie Maßnahmen, die je nach Art der Daten und ihrer Verwendung geeignet sind,

1. Unbefugten den Zugang zu den Verarbeitungsanlagen zu verwehren (*Zugangskontrolle*),

2. zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können (*Datenträgerkontrolle*),

3. die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter Daten zu verhindern (*Speicherkontrolle*),

4. zu verhindern, dass Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten benutzt werden können (*Benutzerkontrolle*),

5. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (*Zugriffskontrolle*),

6. zu gewährleisten, dass überprüft und festgestellt werden kann, welche Daten zu welcher Zeit an wen übermittelt worden sind (*Übermittlungskontrolle*),

7. zu gewährleisten, dass überprüft und festgestellt werden kann, welche Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind (*Eingabekontrolle*),

8. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (*Verfügbarkeitskontrolle*),

9. zu gewährleisten, dass Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen der Auftraggeber verarbeitet werden können (*Auftragskontrolle*),

10. zu gewährleisten, dass bei der Übertragung von Daten sowie beim Transport von Datenträgern diese nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können (*Transportkontrolle*),

11. die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird (*Organisationskontrolle*).

VII. Inkrafttreten

Diese Leitlinie tritt am Tage nach der Veröffentlichung in den Amtlichen Mitteilungen der Carl von Ossietzky Universität Oldenburg in Kraft.