UNIVERSITÄT DES SAARLANDES

Handreichung zur Datenablage dienstlicher Daten und Informationen

Behördlicher Datenschutzbeauftragter/IT-Sicherheitsbeauftragter | 31.01.2022

Einleitung

Diese Handreichung soll den Nutzerinnen und Nutzern der IT-Ressourcen der UdS Hilfestellung beim Umgang mit elektronischen Daten und Informationen im Rahmen ihrer dienstlichen Tätigkeit (Forschung und Lehre, Verwaltung) geben. So werden die verschiedenen Möglichkeiten der Speicherung von Daten und Informationen auf den von der UdS zur Verfügung gestellten Speicherdiensten, sowohl im Bereich der UdS als auch im Internet (Cloud), und die dabei zu beachtenden Anforderungen dargestellt.

Bei der Speicherung elektronischer Daten treten zwei Fragen in den Vordergrund, nämlich nach der Art des verwendeten Speichers und nach den rechtlichen Belangen, die berücksichtigt werden müssen. Für die Antwort auf beide Fragen ist insbesondere der Informationsinhalt entscheidend.

1 Arten von Speicherdiensten

Den Nutzerinnen und Nutzern stehen verschiedene Möglichkeiten zur Speicherung von Daten und Informationen zur Verfügung:

- Lokale Festplatte des persönlichen PC (Desktop, Notebook usw.)
- Netzlaufwerke auf File-Servern des Hochschul-IT-Zentrums oder der dezentralen Organisationseinheiten (HIZ-FS)
- Cloud-Speicherdienste in Microsoft 365 (OneDrive, SharePoint)
- Cloud-Speicherdienst des Hochschul-IT-Zentrums (HIZCloud)

Die aufgeführten Speicherdienste unterscheiden sich vor allem hinsichtlich der Möglichkeiten, auf die gespeicherten Daten unabhängig vom Aufenthaltsort der Nutzenden zugreifen. So eignen sich für die kollaborative Bearbeitung von Daten und den gemeinsamen Zugriff auf Daten und Informationen die oben aufgeführten Cloud-Speicherdienste MS 365 und HIZCloud, während die Speicherung von Daten und Informationen auf Netzlaufwerken nur das Teilen von Daten innerhalb der Arbeitsgruppe erlauben und ein gemeinsames Arbeiten an Dokumenten nicht möglich ist.

Des Weiteren unterscheiden sich die aufgeführten Speicherdienste hinsichtlich des Standorts der Speicherung der Daten. Während sich die lokalen Festplatten des Desktop-PC oder Notebooks, die Fileserver des HIZ-FS und die HIZCloud im Herrschaftsbereich der UdS befinden, handelt es sich bei den Speichermöglichkeiten von MS 365 um eine sog. Public Cloud, welche durch einen externen Dritten (Microsoft) betrieben wird. Die UdS hat durch technische und organisatorische Maßnahmen sichergestellt, dass eine Nutzung von MS 365 beim Umgang mit dienstlichen Daten möglich ist. U.a. wurde eine Vereinbarung über die Auftragsverarbeitung unter Einbeziehung der aktuellen Standardvertragsklauseln der Europäischen Kommission und Geheimhaltungsvereinbarungen abgeschlossen. In diesen Vertragswerken ist vertraglich vereinbart, dass Daten in Rechenzentren gespeichert und verarbeitet werden, die im Geltungsbereich der Datenschutz-Grundverordnung

(Europäischer Wirtschaftsraum) oder in Staaten, für die ein den Vorgaben der Datenschutz-Grundverordnung entsprechendes Datenschutzniveau aufweisen, lokalisiert sind.

Grundsätzlich ist zu beachten, dass unabhängig von der Speichermöglichkeit der Zugriff auf die Daten und Informationen auf die Personen beschränkt werden sollte, welche die Daten und Informationen für ihre dienstliche oder wissenschaftliche Tätigkeit benötigen. Dies gilt insbesondere für den Umgang mit personenbezogenen Daten. Für personenbezogene Daten sind neben den Hinweisen in dieser Handreichung die Vorgaben der Datenschutz-Grundverordnung (DSGVO), des Saarländischen Datenschutzgesetzes (SDSG) sowie einschlägiger datenschutzrechtlicher Vorschriften § 22 SDSG, §§ 95ff Saarländisches Beamtengesetz für die Verarbeitung von Beschäftigtendaten, zu beachten. Bei jeder Verarbeitung und somit auch bei der Speicherung personenbezogener Daten ist auf den **Grundsatz der Datenminimierung** und den **Grundsatz der Speicherbegrenzung zu achten**, was bedeutet, dass nur die personenbezogenen Daten erhoben, gespeichert und verarbeitet werden dürfen, die für die jeweilige Aufgabenstellung oder **Aufgabenerfüllung unbedingt benötigt werden** und dass die personenbezogenen Daten, sobald der Zweck der Verarbeitung es zulässt, **gelöscht** oder **anonymisiert** werden müssen.

Ein hoher oder sehr hoher Schutzbedarf auch von Daten und Informationen ohne Personenbezug kann sich aus vertraglichen Vereinbarungen (Geheimhaltungsvereinbarungen) oder gesetzlichen Vorschriften (Verschlusssachen-Verordnung) ergeben.

2 Schutzbedarf

Für die Entscheidung, welche Speichermöglichkeit für Aufbewahrung der Daten und Informationen gewählt wird, kommt es auf den Schutzbedarf der Daten und Informationen an. Der Schutzbedarf von Daten und Informationen wird in die drei Kategorien „normal“, „hoch“ und „sehr hoch“ eingeteilt. Die folgende Tabelle soll eine grobe Orientierung geben:

Ursprung der Daten und Informationen	Schutzbedarfskategorie
Daten aus öffentlich zugänglichen Quellen	normal
Allgemeine Daten aus dem Bereich der Lehre (Vorlesungsunterlagen, Präsentationen, Versuchsanleitungen)	normal
Dienstliche, nicht wissenschaftliche Daten aus den Bereichen Lehre (Prüfungsergebnisse, Gutachten, Klausuren, Lehrplanung) und	hoch bis sehr hoch

Verwaltung (Haushaltsdaten, Leistungsbeschreibungen, Verträge)	
Wissenschaftliche personenbezogene Daten mit offener Lizenz (Open Data)	keinen
Wissenschaftliche personenbezogene Daten, sofern sie für Dritte nicht interpretierbar sind	normal bis hoch
Wissenschaftliche personenbezogene Daten (z.B. Untersuchungsergebnisse, Messreihen)	hoch bis sehr hoch
Personalaktendaten	sehr hoch

Der Schutzbedarf wird anhand der drei Schutzziele der IT-Sicherheit **Verfügbarkeit**, **Integrität** und **Vertraulichkeit** bestimmt. Der Schutzbedarf bestimmt die Eignung der Daten und Informationen für die Speicherung in den Speicherdiensten. Es ist wichtig, dass Sie sich schon beim Erstellen der Dateien über deren Schutzbedarf Gedanken machen. Für den Fall, dass Sie z.B. mit einem Drittmittelgeber eine Geheimhaltungsregelung vereinbart haben, muss diese auch beim Ablagekonzept berücksichtigt werden. Grundsätzlich sind lokale Speicherdienste und MS365 für die Ablage von Daten und Informationen mit normalem, hohem und sehr hohem Schutzbedarf geeignet. Für die Ablage von Daten und Informationen mit sehr hohem Schutzbedarf sollten aber vorzugsweise strukturierte Ablagesysteme wie das DMS oder spezielle Systeme, bspw. für klinische Studien genutzt werden. Außerdem kann das Schutzniveau der Daten und Informationen mit hohem oder sehr hohen Schutzbedarf durch zusätzliche Maßnahmen, wie die Verschlüsselung der Daten erhöht werden.

3 Allgemeine Anforderungen

3.1 Nutzung anderer Speicherdienste

Die Nutzung von Speicherungsmöglichkeiten mittels anderer frei verfügbarer Cloud-Dienste (z.B. Dropbox, Amazon Drive, iCloud, Google Drive, Magenta, gmx usw.) sollte für die Speicherung dienstlicher Daten und Informationen unterbleiben. Vor der Nutzung solcher Dienste müssen bei der geplanten Speicherung personenbezogener Daten vertragliche Vereinbarungen, sog. Vereinbarung über die Auftragsverarbeitung, mit dem Anbieter geschlossen werden. Dies kann nur durch das zuständige Mitglied des Präsidiums erfolgen. Außerdem ist die für den Datenschutz zuständige Person vor der Nutzung einzubeziehen.

3.2 Verantwortlichkeit

Unabhängig vom genutzten Speicherdienst verbleibt die Verantwortlichkeit für den Umgang mit den Daten und Informationen beim Besitzer der Daten und Informationen. Die nachfolgenden Anforderungen müssen vom Besitzer beachtet und entsprechende Maßnahmen umgesetzt werden.

3.3 Zugriffsberechtigungen

Bei jeder Speicherung von Daten und Informationen ist darauf zu achten, dass durch die Einrichtung von Zugriffsberechtigungen sichergestellt wird, dass nur solche Personen auf die Daten und Informationen zugreifen können, die diese Daten und Informationen für ihre Aufgabenerfüllung benötigen.

3.4 Speicherdauer

Daten und Informationen unterliegen in vielen Fällen einer Löschverpflichtung, sei es durch gesetzliche Regelungen (personenbezogene Daten) oder Aufbewahrungsfristen (abgaben- und steuerrechtliche Vorgaben). Schon bei der Erhebung der Daten sollte festgelegt werden, wie lang die Daten und Informationen vorgehalten bzw. wann sie gelöscht werden müssen. Nähere Einzelheiten zu Aufbewahrungs- und Speicherfristen sind im Kapitel 4 dieses Dokuments dargestellt.

3.5 Datensparsamkeit

Bei der Verarbeitung von personenbezogenen Daten ist der Grundsatz der Datenminimierung zu beachten, d.h. die Erhebung personenbezogener Daten ist auf das für den angestrebten Zweck notwendige Maß zu beschränken.

3.6 Rechtliche und universitäre Vorgaben

Insbesondere für den Umgang mit Daten und Informationen, welche im Rahmen der Verwaltung der UdS verarbeitet werden (Personaldaten, Studierendendaten, Haushaltsdaten), können besondere Regelungen gelten, bspw. hinsichtlich Aufbewahrungs- und Löschfristen und Revisionssicherheit. Diese sind immer zu beachten. Im Zweifelsfall muss die Speicherung mit dem jeweiligen Vorgesetzten, ggf. unter Einbeziehung der/des behördlichen Datenschutzbeauftragten, geklärt werden.

4 Aufbewahrungs- und Löschfristen

Beim Arbeiten mit Dokumenten, unabhängig davon, ob diese in analoger oder digitaler Form vorliegen, stellt sich stets die Frage, wie lange muss oder darf man diese Dokumente aufbewahren.

Bei der Verarbeitung von personenbezogenen Daten ist immer der Grundsatz der Speicherbegrenzung (Art. 5 Abs. 1 lit. e) DSGVO) zu beachten, wonach personenbezogene Daten nur solange in einer Form verarbeitet werden dürfen, welche die Identifizierung der betroffenen Personen ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Das bedeutet, dass personenbezogene Daten nach Wegfall des Verarbeitungszwecks zu anonymisieren oder zu löschen sind. Eine dauerhafte Speicherung personenbezogener Daten ist somit in den meisten Fällen ausgeschlossen.

Hinsichtlich der Aufbewahrung von dienstlichen Dokumenten ist zwischen Aufbewahrungs- und Löschfristen zu unterscheiden. Während die Aufbewahrungsfrist bestimmt, wie lang Dokumente mindestens aufzubewahren sind, legt die Löschfrist den maximalen Aufbewahrungszeitraum fest.

Diese Handreichung soll insbesondere den **dezentralen Bereichen** der Universität des Saarlandes eine Hilfestellung beim rechtskonformen Umgang mit dienstlichen Dokumenten geben.

In der folgenden Tabelle werden für typischerweise in dezentralen Bereichen der Universität des Saarlandes anfallende Dokumentarten die zu beachtenden Aufbewahrungs- und Löschfristen dargestellt:

Dokumententyp	Aufbewahrungs-frist[1]	Löschfrist	Bemerkung
arbeits-/dienstrechtliche Unterlagen			
Bewerbungs-unterlagen	Sechs Monate nach Absage	gleich der Aufbe-wahrungs-frist	Bewerberinnen und Bewerber haben die Möglichkeit, die Besetzungs-entscheidung anzugreifen, daher muss die Klagefrist abgewartet werden.[2] Mit Einwilligung der Bewerberinnen und Bewerber können die Unterlagen auch über die Löschfrist hinaus aufbewahrt werden, bspw. für spätere Besetzungen von in absehbarer Zeit freiwerdenden Stellen.

[1] Aufbewahrungsfristen beginnen, soweit nicht ausdrücklich etwas anderes bestimmt ist, mit dem Ablauf des Jahres, in dem die Vorgänge geschlossen worden sind.

[2] Bei Konkurrentenstreitigkeiten müssen die Daten bis zum Zeitpunkt einer rechtskräftigen Entscheidung über die Bewerberauswahl aufbewahrt werden.

			In der Regel werden die Bewerbungsunterlagen im Dezernat P verwaltet und sollten dezentral direkt nach Abschluss des Verfahrens gelöscht werden.
Kopien von Arbeitsverträgen		Spätestens mit Ausscheiden des Beschäftigten aus dem Dienst	Sollten in dezentralen Bereichen nicht aufbewahrt werden!
Dienstreiseabrechnungen	unterschiedliche Fristen		Löschung in den Sekretariaten sechs Monate nach Entscheidung über die Reisekosten. Nach Digitalisierung des Antrags- und Abrechnungsprozesses sollte auf die dezentrale Aufbewahrung von Unterlagen verzichtet werden.
Arbeitsunfähigkeitsbescheinigungen, Gesundheitsdaten	Übermittlung AU-Bescheinigung unverzüglich an Dezernat Personal	Nach Genesung sollten die Daten im dezentralen Bereich datenschutzgerecht gelöscht werden.	Sämtliche Korrespondenz mit der/dem erkrankten Beschäftigten im Zusammenhang mit der Erkrankung sollte nur in Dezernat Personal aufbewahrt werden.
Unterlagen aus dem Bereich Lehre und Studium[3]			
Prüfungsarbeiten (Klausuren, Zeichnungen usw.), sofern für Endnote relevant	Mind. 1 Monat nach Bekanntgabe der Note. Empfehlung: zwei Jahre nach	Fünf Jahre	Bis max. fünf Jahre nach Prüfungsdatum kann die Prüfungsleistung von Seiten der Universität aberkannt werden (z.B. bei Täuschung)[4]

[3] Bitte beachten Sie auch die Vorgaben der Studentendaten-Verordnung und der Aufbewahrungsrichtlinie der UdS

[4] Bei Rechtsstreitigkeiten über Prüfungsergebnisse müssen die Daten bis zum Zeitpunkt einer rechtskräftigen Entscheidung aufbewahrt werden.

	Bekanntgabe der Note.		
Auflistungen von Prüfungs-ergebnissen in Tabellen, Excel-Dateien u.ä.	Zwei Jahre nach Bekanntgabe der Noten.	Fünf Jahre	
Videos von Vorlesungen		Wenn Studierende oder Gäste aufgezeichnet wurden: Nach Ende der Veranstaltung	Ausnahme: Es gibt didaktische Gründe, die eine längere Speicherung rechtfertigen. Datenschutz beachten: Bei Gästen muss die Einwilligungen der aufgenommenen Personen muss vorliegen!
Bewerberdaten, sofern die Bewerber*innen eine Zulassung erhalten haben		spätestens zehn Jahre nach Ablauf des Bewerbungssemesters zu löschen	Außerhalb des zentralen Campusmanagement-Systems gespeicherte Bewerberdaten sollen unmittelbar nach Abschluss des Vergabeverfahrens gelöscht werden (ggf. unter Beachtung laufender Widerspruchsfristen)
Studierendendaten		spätestens nach Ablauf von 50 Jahren zu löschen	Alle übrigen Daten der Einschreibung oder der Aufnahme in die Hochschule und des Studiums sind nach 15 Jahren nach der Exmatrikulation bzw. der Beendigung des Studiums zu löschen
Alle personenbezogenen Daten, die nicht in die obigen Kategorien fallen		müssen innerhalb von 2 Jahren nach ihrer Erhebung gelöscht werden	z.B. Bewerberdaten und -unterlagen, die nicht zu einer anschließenden Immatrikulation führten
Abschlussdokumente, Akten zu Promotions- und Habilitationsverfahren und Verwaltungsakte		sollten fünf Jahre nach dem Abschluss/der Exmatrikulation gelöscht werden	
Forschungsdaten			

Forschungsdaten	mindestens 10 Jahre		Bei personenbezogenen Daten ist die Aufbewahrungsfrist auch als Löschfrist anzusehen.
Finanzunterlagen bei Drittmittelvorhaben	Festlegung durch Zuwendungsbescheid oder vertraglich Regelung	Regelmäßig nach 10 Jahren	Rechnungen, Time-Sheets, Dienstreiseabrechnungen, Verwendungsnachweise u.ä. sollten dezentral 2 Jahre Projektende gelöscht werden.[5]
Finanzdaten			
Zahlungsbegründende Unterlagen	10 Jahre	Dezentral wird eine Löschung / Vernichtung nach 2 Jahren empfohlen.	Ausgangs- und Eingangsrechnungen, Buchungsbelege[5].
Sonstige Dokumente			
E-Mail		Regelmäßig nach spätestens zehn Jahren, soweit kein berechtigtes Interesse an längerer Speicherung vorliegt.	Da es sich bei E-Mails in den meisten Fällen um personenbezogene Daten handelt, sollte regelmäßig geprüft werden, ob die Dokumente gelöscht werden können.
Sonstige Dokumente		ein Jahr[6]	(sog. Weglegesachen)

Die dargestellten Beispiele stellen die Umsetzung des Grundsatzes der Speicherbegrenzung in Einzelfällen dar. Die Auflistung ist nicht abschließend. Es bedarf für jede Art von Dokumenten einer Einzelfallentscheidung unter Beachtung gesetzlicher und inneruniversitärer Regelungen. Im Zweifelsfall wenden Sie sich bitte an die/den behördlichen Datenschutzbeauftragten.
Im Zusammenhang mit der Verarbeitung personenbezogener Daten weisen wir außerdem auf den Grundsatz der Vertraulichkeit hin. Danach dürfen auf personenbezogene Daten nur die Beschäftigten Zugriff haben, welche diese Daten für die Erfüllung Ihrer dienstlichen Aufgaben benötigen.

[5] Originalbelege werden zentral in Dezernat HF aufbewahrt und nach Ablauf der Aufbewahrungsfristen gelöscht/vernichtet

[6] Das Jahresende sollte regelmäßig zum Aussondern von nicht mehr benötigten Dokumenten und Unterlagen genutzt werden.