Der Landesbeauftragte für den
DATENSCHUTZ und die
INFORMATIONSFREIHEIT
Rheinland-Pfalz

Begriffsbestimmungen, § 3 LDSG / Art. 4 und 9 DS-GVO

personenbezogene Daten

Name, Anschrift, Geb.-Datum als unmittelbar identifizierende Daten

Zusammenfassung mehrerer sog. personenbeziehbarer Daten wie Staatsangehörigkeit, Alter oder Geschlecht kann zur Identifizierung einer Person führen

Angaben Verstorbener oder über juristische Personen und Personenmehrheiten sind durch das LDSG grundsätzlich nicht geschützt.

Aber: Namen von Einzelkaufleuten oder einer Ein-Mann-GmbH

Verarbeitung in mehreren Phasen wie das
Erheben, Erfassen, Löschen, Vernichten, die Bereitstellung oder Verwendung

Besondere Kategorien personenbezogener Daten
u.a. Herkunft, politische Meinung, Gesundheit, genetische und biometrische Daten

Rechtmäßigkeit der Datenverarbeitung, § 5 LDSG / Art. 6 Abs. 1 a, f DS-GVO

Erlaubnis oder Anordnung durch Gesetz

oder

Einwilligung der Betroffenen

Prinzip der informierten Einwilligung (§ 5 Abs. 2 LDSG / Art. 7, 13 DS-GVO), d.h. sie ist nur wirksam, wenn u.a. auf Folgendes hingewiesen wird:

- Einwilligung beruht auf der freien Entscheidung
- Ablehnung der Einwilligung oder deren jederzeitiger Widerruf ist nicht mit Nachteilen verbunden
- Möglicher Empfängerkreis und Zweck der Verarbeitung
- Verantwortliche Stelle für die Datenverarbeitung

Ansonsten Verarbeitungsverbot personenbezogener Daten!

Ausnahme: Informationen über die Tätigkeiten von Amtsträgern in Ausübung ihres Amtes, soweit diese Tätigkeiten Außenwirkung haben. Amtsträger (z.B. Mitarbeiter einer öffentlichen Stelle, Ratsmitglieder) als für den Staat handelnde Personen können sich dabei grds. nicht auf das Recht der informationellen Selbstbestimmung berufen.

Verarbeitung von Daten (§§ 12 – 14 LDSG)

Voraussetzungen:

Kenntnis der Daten ist zur rechtmäßigen Erfüllung der Aufgaben der verantwortlichen Stelle **erforderlich (Art. 5 Abs. 1 c DS-GVO)**

Erforderlichkeit heißt, dass die personenbezogenen Daten unabdingbar sein müssen, damit die verantwortliche Stelle die Aufgaben erfüllen kann.

Speichern oder Verwenden im Rahmen des Zwecks, für den die Daten erhoben wurden – **Zweckbindung (Art. 5 Abs. 1 b DS-GVO)**

Funktionaler Verwaltungsbegriff, d.h. funktional unterschiedliche Bereiche der Hochschulverwaltung sind im Hinblick auf die Datenverarbeitung voneinander getrennt zu betrachten.
Weitergabe personenbezogener Daten bspw.

- von Personal- an Studierendenverwaltung
- zwischen Fachbereichen
- von Standort Koblenz nach Standort Landau

ggf. nur mit rechtlicher Grundlage zulässig.

Mailing-Aktion

Um eine Informationsveranstaltung zu bewerben, versendet das Alumni-Referat einen Flyer per E-Mail an über 100 Mitarbeiterinnen und Mitarbeiter privater Organisationen. Dabei werden alle Adressen in das „An:“ – bzw. „cc:“ – Feld geschrieben. Somit sieht jeder Empfänger der E-Mail, wer die Nachricht noch alles erhalten hat.

Ist das datenschutzrechtlich zulässig?

Wie fällt Ihre Bewertung aus, wenn eine solche E-Mail an die personalisierten Anschriften von Mitarbeiterinnen und Mitarbeitern verschiedener Hochschulverwaltungen ginge?

Mailing-Aktion

personenbezogen	Mailadressen natürlicher Personen mit Vor- und Nachname
Form der Datenverarbeitung	Übermittlung an nicht-öffentliche Stellen bzw. natürliche Personen
Rechtsgrundlage	§ 16 Abs. 1 LDSG / Art. 6 Abs. 1e, Abs. 3 DS-GVO zur Aufgabenerledigung aber nicht erforderlich Datenminimierung
Besser	Versand einer E-Mail an großen Empfänger-kreis per „bcc:“- Feld In das „An:“- Feld die eigene E-Mail-Adresse eintragen
Tipp	Datenschutz-Tipp 7 der **T**echnischen **H**ochschule **M**ittelhessen: „Die häufigsten E-Mail-Ärgernisse Vermeiden!“

Mailing-Aktion

personenbezogen	Mailadressen natürlicher Personen mit Vor- und Nachname und Dienststelle
Form der Datenverarbeitung	Übermittlung an öffentliche Stellen
„Rechtsgrundlage“	Amtsträgertheorie

Angaben, die im Zusammenhang mit einer nach außen gerichteten Tätigkeit als Amtsträger stehen, sind Name, Vorname, Amtsbezeichnung sowie die Erreichbarkeits-angaben.

Diese Daten können ohne Einwilligung des Betroffenen oder eine Rechtsgrundlage übermittelt werden, d.h. deren Veröffentlichung ist nicht mit den Mitteln des Datenschutzes angreifbar.

Im Einzelfall ist Fürsorgepflicht zu berücksichtigen.

Anders bei Informationen des Grundverhältnis, z.B. Lichtbild, Geburtsdatum, private Anschrift.

Elektronische Übermittlung personenbezogener Daten

Eine Behörde möchte Lichtbilder aus dem Pass- und Personalausweisregister auf Anfrage einer Bußgeldstelle über öffentlich zugängliche Netze unverschlüsselt versenden.

Wie sehen Sie das?

Elektronische Übermittlung personenbezogener Daten

Eine unverschlüsselte E-Mail ist, was den Schutz des Inhalts vor der Kenntnisnahme und Veränderung durch unbefugte Dritte angeht, mit einer mit Bleistift geschriebenen Postkarte zu vergleichen – sie kann abgefangen, mitgelesen und inhaltlich verändert werden. Absender und Empfänger können nie sicher sein, mit wem sie kommunizieren.

personenbezogen	Lichtbild und weitere Information zur Person
Form der Datenverarbeitung	Übermittlung zwischen öffentlichen Stellen
Rechtsgrundlage	§ 14 LDSG / Art. 6 Abs. 1e, Abs. 3 DS-GVO aber Unverschlüsselte Übermittlung personenbezogener Daten per E-Mail über das Internet ist rechtswidrig, da eine unbefugte Kenntnisnahme Dritter nicht ausgeschlossen ist. § 9 Abs. 2 Nr. 4 LDSG / Art. 32 Abs. 1 DS-GVO

Elektronische Übermittlung personenbezogener Daten

entweder

sichere Infrastruktur (KNRP, rlp-netz, virtuelle Poststelle) nutzen

oder

passwortgeschützte pdf-Dateien oder Archiv-Container (Zip-Container) verwenden.

Das Passwort ist der empfangenden Stelle auf einem separaten Weg gesondert zu übermitteln.

https://www.datenschutz.rlp.de/de/themenfelder-themen/e-mail-inhalte-schuetzen/

Verwendung von Terminplanern

Die Verwendung von „**doodle**“ als ein im Ausland ansässiger Online-Dienst wird kritisch gesehen.

Die dienstliche Nutzung unter bestimmten Voraussetzungen zulässig

http://www.datenschutz.rlp.de/downloads/misc/FAQ-Doodle.pdf

Alternativen zu "doodle" sind zu finden unter

https://dudle.inf.tu-dresden.de/privacy/

mit ausführlicher Beschreibung zur Bedienung und zum Verschlüsselungskonzept

sowie unter

https://terminplaner.dfn.de/

Unter https://www.dfn.de/dienstleistungen/dfnterminplaner/ wird der Dienst erläutert.

Umgang mit Passwörtern

Dürfen Passwörter für den Einblick in das Studierenden- und Prüfungsverwaltungssystem an Kolleginnen und Kollegen, z.B. für dienstliche Zwecke, weitergereicht werden?

Umgang mit Passwörtern

Nein, es gilt das Prinzip der Einzelkennung.

Zugangskontrolle gemäß § 9 Abs. 2 Nr. 2 LDSG / Art. 32 Abs. 1 DS-GVO

Dies dient auch der Nachvollziehbarkeit der Protokollierung.

Verarbeitungskontrolle gemäß § 9 Abs. 2 Nr. 10 LDSG / Art. 32 Abs. 1 DS-GVO

Nur ausnahmsweise, in besonders dringlichen Fällen darf eine Kennung

einem Vertreter mitgeteilt werden.

Danach ist ein neues Passwort zu vergeben.

Aufbewahrung von Akten

Ist es datenschutzkonform, z.B. eine Prüfungsakte eines Studierenden, die personenbezogene Daten enthält, offen zugänglich im Büro liegen zu lassen?

Aufbewahrung von Akten

Grundsätzlich handelt es sich um ein Offenbaren von Daten, sofern Dritte Einsicht nehmen können.

Innerhalb der verantwortlichen Stelle, also wenn eine Kollegin bzw. ein Kollege Einsicht nehmen könnte, würde es sich um eine Nutzung von Daten, evtl. verbunden mit einer Zweckänderung, handeln.

Funktionaler Verwaltungsbegriff, vgl. Folie 6

Es sind Maßnahmen zu treffen, die verhindern, dass Unbefugte auf diese Daten zugreifen können (§ 9 Abs. 4 LDSG / Art. 32 Abs. 1 DS-GVO), insbesondere sind Diensträume bei Abwesenheit zu verschließen.

Aufbewahrung von Akten

Vorkehrungen gegenüber Reinigungskräften, unabhängig davon, ob internes oder externes Reinigungspersonal eingesetzt wird:

Reinigung außerhalb der Dienstzeit – Akten sind einzuschließen

Reinigung während der Dienstzeit – grds. genügt die bloße Anwesenheit des Beschäftigten

Auch Besucher und Kollegen aus anderen Fachbereichen sind also ggf. als Unbefugte anzusehen, gerade wenn es um besondere Amtsgeheimnisse wie z.B. das Personalgeheimnis geht.

Nutzung sozialer Medien

Problematisch ist hier, dass die öffentliche Stelle damit z.B. für Facebook wertvolle Nutzungsdaten erzeugt .

Erforderlichkeitsprüfung
Soziales Medium sollte nur genutzt werden, wenn eine Prüfung ergeben hat, dass ohne eine solche Präsenz erhebliche Nachteile drohen bzw. die Aufgabenerfüllung der z.B. Alumniabteilung ernsthaft beeinträchtigt wäre.

Daher vorrangig nur Informationsmedium zur Verstärkung der Reichweite von Informationsangeboten insbesondere in den Bereichen Kultur/Veranstaltungen

Näheres unter

https://www.datenschutz.rlp.de/de/themenfelder-themen/handlungsrahmen-soziale-netzwerke/

sowie weiterführenden Links.

Verwendung von Bildern

Kunsturhebergesetz (KunstUrhG)

Erfasst werden nur Bildnisse, d.h. die Darstellung einer oder mehrerer Personen, die die äußere Erscheinung der Abgebildeten in einer für Dritte erkennbaren Weise wiedergibt.

§ 22

Bildnisse dürfen grundsätzlich nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden.

Verbreitungsgrad der Informationen im Medium Internet hat deutlich höheren Umfang, als dies bei einer Veröffentlichung bspw. in einer Broschüre oder einer regionalen Tageszeitung der Fall ist. Aufgrund der weltweiten Zugriffsmöglichkeit besteht ein höheres Gefährdungspotential.

§23

Ausnahmen

Weitere Informationen - https://www.lda.bayern.de/media/info_kompakt_fotos.pdf

Muster für eine Einwilligungserklärung für die Veröffentlichung von Fotos
http://www.lfd.niedersachsen.de/portal/live.php?navigation_id=12982&article_id=56127&_psmand=48

Der Landesbeauftragte für den
DATENSCHUTZ und die
INFORMATIONSFREIHEIT
Rheinland-Pfalz

Postanschrift:	Postfach 30 40 55020 Mainz
Büroanschrift:	Hintere Bleiche 34 55116 Mainz
Telefon:	+49 (6131) 208-2449
Telefax:	+49 (6131) 208-2497
E-Mail:	poststelle@datenschutz.rlp.de
Web:	www.datenschutz.rlp.de