eLearning im Dialog GmbH
Mahlower Str. 23/24
D-12049 Berlin

Telefon: 0049 30 50 56 10 70
Telefax: 0049 30 50 59 08 60

Mail: info@eledia.de

Internet: www.eledia.de

Moodle Funktionen zur Umsetzung der DSGVO-Anforderungen

Hinweis zu verwendeten Begrifflichkeiten

Auf der Moodle-Oberfläche werden die Begrifflichkeiten derzeit noch nicht einheitlich genutzt. Synonym werden ‚Richtlinie' und ‚Einwilligung' verwendet. Der Begriff der Einwilligung ist datenschutzrechtlich eindeutig belegt. Die Verarbeitung personenbezogener Daten kann auf verschiedenen Grundlagen legitimiert sein. Dazu gehören u.a. ein Gesetz, ein Vertrag, eine ausdrückliche Einwilligung oder ein berechtigtes Interesse. Wenn ein Vertrag vorliegt, ist es nicht erforderlich, dass ein betroffener Nutzer eine Einwilligung zur Verarbeitung erteilt. Der Vertrag regelt das. Wenn man die Person nun auffordert, die Einwilligung zu erteilen, kann sie die Einwilligung auch wieder widerrufen. Damit ist jedoch unklar, was mit den Regelungen aus dem Vertrag wird.

Ein Nutzer, dessen Daten auf Grundlage eines Vertrages verarbeitet werden, muss gleichwohl über die Verarbeitung und die damit verbundenen Rechte informiert werden und dieses bestätigen.

Um dem betroffenen Nutzer größtmögliche Klarheit zu verschaffen, sollte der Begriff Einwilligung nicht genutzt werden, wenn die Verarbeitung der Daten auf Grundlage eines Vertrages beruht.

Die Situation kann nun noch komplizierter werden, wenn eine Plattform von Anwendern genutzt wird, für die unterschiedliche Grundlagen gelten. Ein Beispiel dazu: Die Plattform wird von Mitarbeitern und Kunden genutzt. Während die Mitarbeiterdatenverarbeitung durch den Arbeitsvertrag legitimiert ist, erteilen Kunden ihre individuelle Einwilligung.

Leider haben wir noch keine überzeugende Begrifflichkeit gefunden, die für die verschiedenen Situationen passt. Vermutlich wird es daher im offiziellen deutschen Sprachpaket noch zu Änderungen der Begrifflichkeit kommen.

Sie haben für Ihr Moodle-System die Möglichkeit, die Begriffe in der Sprachverwaltung so anzupassen, dass Sie für Ihren Einsatzzweck optimal sind.

Stand: 1. Juni 2018

Inhaltsverzeichnis

1 Übersicht

Lernplattformen speichern von ihren Nutzern eine Vielzahl von Daten. Manche Datenspeichervorgänge sind offensichtlich, manche nur gut nachvollziehbar, wenn man die komplexen Prozesse durchschaut. Die Datenschutzgrundverordnung erhöht die Ansprüche an alle Beteiligten. Höchstes Ziel ist es sicherzustellen, dass ein betroffener Nutzer, dessen Daten verarbeitet werden, keine Nachteile erfährt. Der Betroffene soll daher über die Zwecke der Speicherung von Daten über ihn und den Umfang der Datenspeicherung informiert sein. Zudem hat er das Recht, Daten löschen zu lassen, mitzunehmen oder einfach einen Bericht zu erhalten, welche Daten gespeichert werden.

Verbunden ist dies immer mit der Aufforderung, den Betroffenen aktiv über seine verschiedenen Rechte aufzuklären.

Damit dies mit Hilfe der Lernplattform Moodle gelingt, sind verschiedene Funktionen bereitgestellt worden. Dazu gehören:

- Information des Nutzers über die Grundlagen der Verarbeitung und seine Rechte. In manchen Fällen muss erst noch die Einwilligung eingeholt werden. In anderen Fällen reicht die Information. In jedem Fall muss dieser Vorgang dokumentiert werden.
- Der Nutzer soll leicht seine Rechte wahrnehmen können. Dazu muss er die verantwortlichen Ansprechpartner kontaktieren können, um Fragen zu stellen, Berichte anzufordern bzw. Löschvorgänge zu initiieren.
- Die o.g. Vorgänge müssen dann abwickelbar sein.
- Wenn Nutzer sich selber registrieren, muss sichergestellt werden, dass sie 16 Jahre oder älter sind. Dieser Vorgang wurde für die Selbstregistrierung ergänzt.
- Für die gespeicherten Daten muss ein Aufbewahrungszeitraum definierbar sein. Das Löschen von Daten, die diesen Zeitraum überschritten haben, muss ermöglicht werden.

Seit Frühjahr 2017 ist für Moodle an der Umsetzung dieser Anforderungen gearbeitet worden. Im Mai 2018 sind entsprechende Funktionen bereitgestellt worden.

2 Kommunikation mit den Datenschutzansprechpersonen

Die Nutzer der Lernplattform haben u.a. das Recht, Auskünfte über die gespeicherten Daten zu erhalten oder Daten löschen zu lassen. Dazu brauchen Sie einen Ansprechpartner. Sie haben in Moodle die Möglichkeit, hierfür eine Rolle anzulegen, Nutzern diese Rolle zuzuweisen, damit sie benachrichtigt werden und die entsprechenden Arbeitsschritte ausführen können.

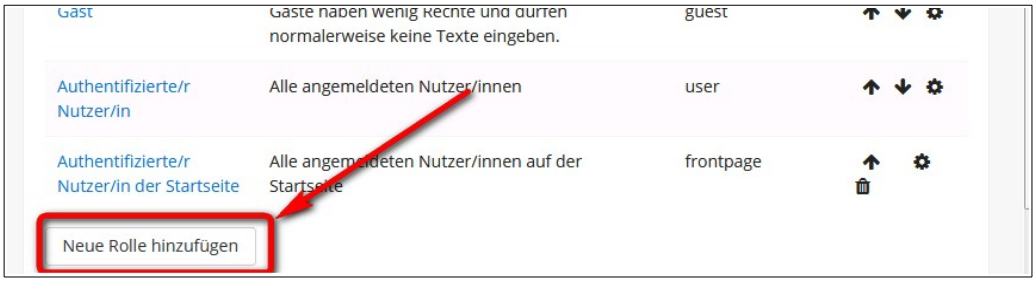
Es ist eine häufige Fehleinschätzung, dass diese Aufgabe vom betrieblichen Datenschutzbeauftragten wahrgenommen wird. Die konkrete Auskunft oder das Löschen wird meist jemand aus dem eLearning-Team übernehmen. Aus diesem Grund empfehle ich auch hier den Begriff Datenschutzbeauftragter zu vermeiden, weil diese Begrifflichkeit eindeutig im Unternehmen Personen zugeordnet sind. Leider verwendet die englische Sprachoberfläche hier den Begriff Data Protection Officer.

Wie gehen Sie vor?

1. Neue Rolle anlegen
2. Nutzern die neue Rolle zuweisen
3. Die neue Funktion aktivieren.

2.1 Neue Rolle für Datenschutzansprechpartner anlegen

Um die Rolle Datenschutzansprechpartner anzulegen, gehen Sie über *Website-Administration→ Nutzer/innen→Rechte ändern→ Rollen verwalten*. Klicken Sie unten auf *Neue Rolle hinzufügen.*



Die folgende Seite können Sie einfach mit ‚Weiter' bestätigen, da Sie keine bestehende Rolle als Grundlage verwenden.

Füllen Sie die Felder zur Bezeichnung der Rolle aus.

Tragen Sie unter ‚Kurzbezeichnung' einen Ein-Wort-Begriff und unter ‚Angepasster Rollenname' den Titel, der angezeigt werden soll, ein.

Als Kontexttyp für diese Rolle wählen Sie „Kernsystem" aus.

Blättern Sie nun herunter bis zur großen Rechte-Tabelle. Das Eingabefeld für Filter ist sehr hilfreich, um die entsprechenden Berechtigungen zu finden. Die Suche beginnt sofort nach der Begriffseingabe.

Suchen Sie nach ‚dataprivacy' und aktivieren Sie folgende Funktionen durch Anklicken von ‚Erlauben'.

- Datenverarbeitung verwalten
- Datenanfragen verwalten
- Datenanfrage für Kinder erstellen (ermöglicht im Namen anderer Nutzer einen Bericht anzufordern oder Daten löschen zulassen).

Suchen Sie nun nach ‚policy'.

- Richtlinien verwalten
- Bericht über Einwilligungen ansehen
- Einwilligung zu den Richtlinien im Namen einer anderen Person (erlaubt im Namen einer anderen Person die Richtlinien zu bestätigen).

Speichern Sie nun die Eingaben durch ‚Neue Rolle erzeugen'.

Falls Sie in Ihrer Plattform den Zugriff von Gästen erlauben und diese ebenfalls datenschutzrechtlich informiert werden sollen, sollten Sie in der Rolle Gast eine zusätzliche Berechtigung setzen.

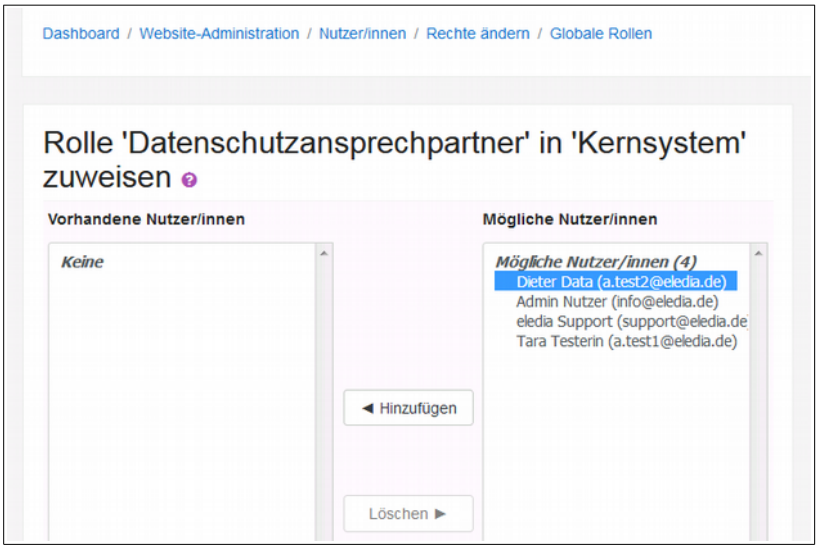
In der Übersicht über die verschiedenen Rollen klicken Sie in der Zeile zur Gastrolle auf das Zahnrad-Icon. Im Filterfeld geben Sie ‚policy' ein. Setzen Sie bei ‚Einwilligung zu den Richtlinien' den Status auf ‚Erlauben' und speichern Sie ab.

2.2 Globale Rolle für Datenschutzansprechpartner vergeben

In diesem Schritt geht es darum, Nutzer festzulegen, die über Anfragen per E-Mail benachrichtigt werden und die entsprechenden Schritte in der Plattform einleiten können.

Sofern die entsprechenden Nutzer auf der Plattform noch nicht angelegt worden sind, sollten Sie dies zuerst tun.

Um einem Nutzer die Rolle Datenschutzansprechpartner zuzuweisen, navigieren Sie zu *Website-Administration→Nutzer/innen→Rechte ändern→Globale Rollen*. Nach Klick auf die neu angelegte Rolle können Sie über eine zweispaltige Ansicht die globale Rolle an Nutzer zuweisen oder Nutzer aus dieser Rolle austragen.



In der Übersicht der Globalen Rollen sehen Sie, welche Nutzer welcher globalen Rolle zugewiesen sind.

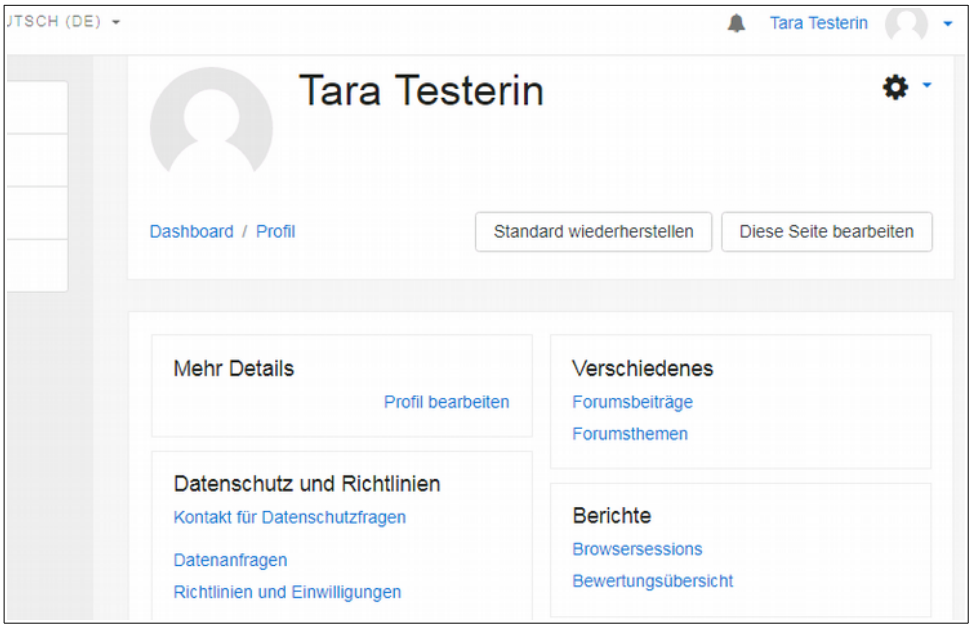
2.3 Die neue Funktion aktivieren

Nachdem Sie die Rolle definiert und Nutzern zugewiesen haben, ist es erforderlich, die Funktion für die Anwender der Plattform zu aktivieren. Dies erfolgt unter *Website-Administration → Nutzer/innen → Datenschutz und Richtlinien → Datenschutzeinstellungen*. Hier sind zwei Häkchen zu setzen unter Kontakt für Datenschutzfragen und Rollenzuordnung des/der Datenschutzansprechpartners.

Beim zweiten Punkt ist die neu angelegte Rolle sichtbar und muss angeklickt werden. Danach müssen die Einstellungen noch gespeichert werden.

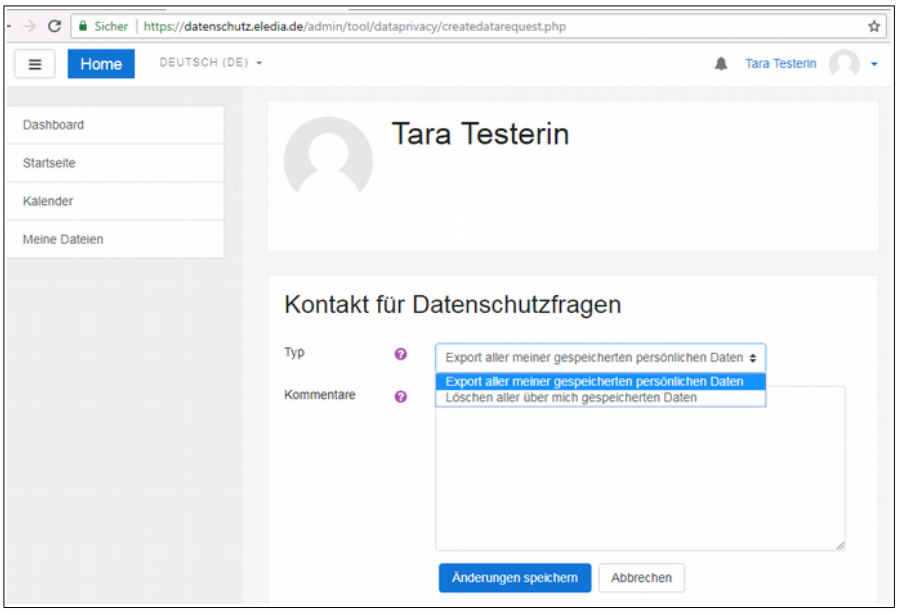
2.4 Anfragen stellen (Nutzersicht)

In seinem Profil kann ein Nutzer Datenanfragen stellen, den Datenschutzansprechpartner kontaktieren oder Einwilligungen einsehen. Die entsprechenden Links sind auf der Profilseite des Nutzers im Bereich „Datenschutz und Richtlinien" direkt sichtbar.



Unter Kontakt wird eine Formular für allgemeine Anfragen bereitgestellt. Die Anfrage wird in Moodle abgelegt und steht den entsprechenden Personen zur Verfügung. Zusätzlich wird sie per E-Mail zugestellt.

In der Option *Datenfragen* lassen sich unter Typ Vorlagen als Betreff bzw. Grund der Anfrage auswählen. Auswählbar ist ein Bericht über die gespeicherten Daten und der Wunsch, dass die Daten gelöscht werden. Im Kommentarfeld kann eine Text dazu eingegeben werden.



Hat die Nutzer eine Datenanfrage versendet, erscheint diese in der Übersicht unter *Datenanfragen.*

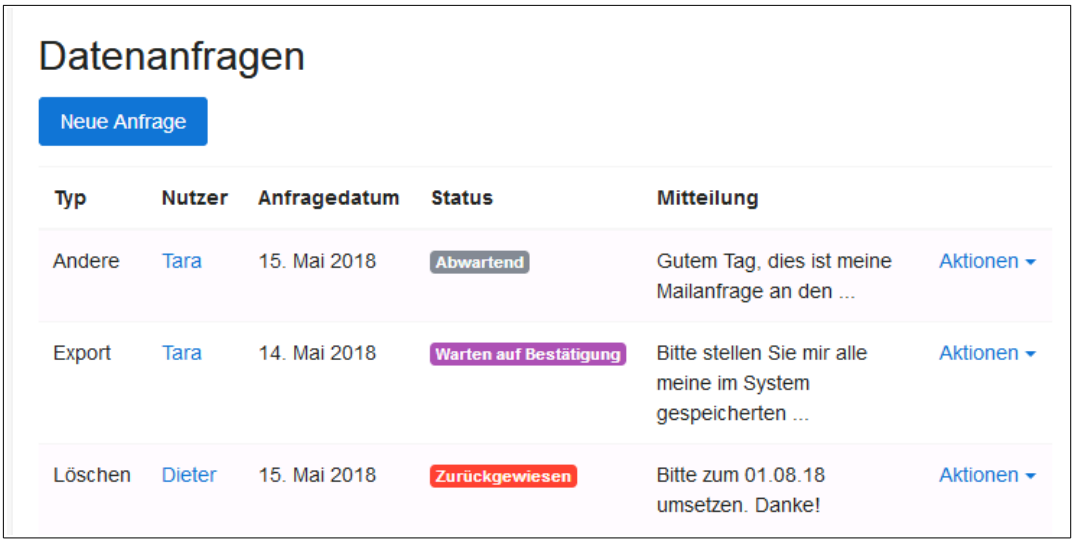
Hier sind sowohl Thema und Datum als auch der Bearbeitungsstatus einsehbar. Die Anfrage kann an

dieser Stelle durch die Nutzer abgebrochen werden.

Unter Richtlinien und Einwilligungen kann von jedem Nutzer der letzte eigene Stand zu Bestätigungen zum Datenschutz eingesehen werden. Die inhaltliche Beantwortung der E-Mails erfolgt über Ihr E-Mailprogramm falls Sie mit dem Nutzer weiter kommunizieren wollen.

2.5 Anfragen bearbeiten

Die Anfragen lassen sich unter W*ebsite-Administration→Nutzer/innen→Datenschutz und Richtlinien→ Datenanfragen* einsehen. Der Typ „Andere" verweist auf eine Kontaktaufnahme per Mail. Unter Aktionen lassen sich Anfragen bestätigen bzw. zurückweisen.



2.5.1 Informationsanfrage

Bei der Informationsanfrage nimmt der Nutzer mit dem Datenschutzansprechpartner Kontakt auf, um Informationen zu erhalten. Mit der Anfrage ist nicht der Wunsch auf einen Bericht oder das Löschen von Daten verbunden.

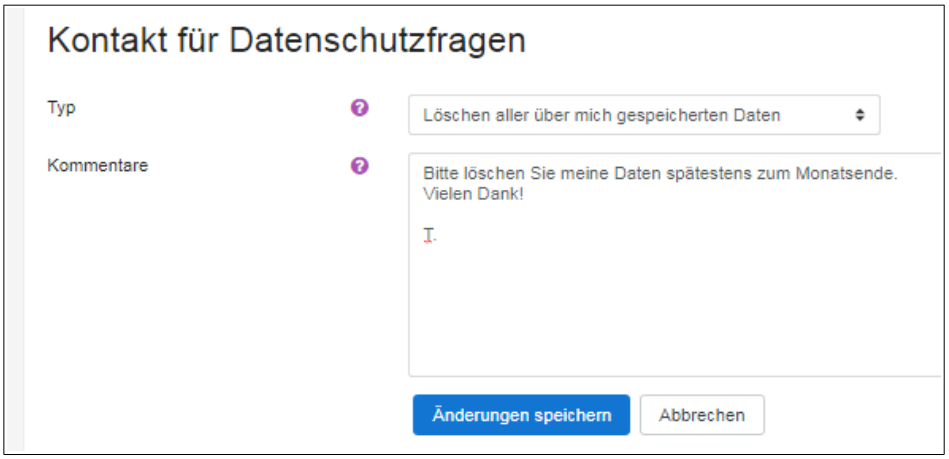
2.5.2 Auskunft über gespeicherte Daten (Bericht/Export)

Der Nutzer kann Zugriff auf die über ihn gespeicherten Daten erhalten. Nach der Bestätigung der Anfrage wird ein Bericht mit einem Datenauszug erstellt. Er enthält alle Daten, die mit dem Benutzer verbunden sind. Der Nutzer kann sich dann eine Zip-Datei herunterladen. Vorläufig wird diese Datei im sog. JSON-Format bereitgestellt. Dabei handelt es sich um ein Bündel von Textdateien mit Feldkennzeichen. Dieses Format erfüllt zugleich die Voraussetzungen für Datenportabilität, da die Daten grundsätzlich maschinenlesbar sind.

Es ist geplant, diese Daten später auch als HTML- oder PDF-Dateien zur Verfügung zu stellen.

2.5.3 Löschanfrage eines Nutzers

Eine Anfrage zur Löschung aller persönlichen Daten kann ein Nutzer über die Option Datenanfragen auf seiner Profilseite stellen. Nach einem Klick auf *Neue Anfrage* wählt der Nutzer dazu den Typ: *Löschen aller über mich gespeicherten Daten* aus. Im Kommentarteil können weitere Bemerkungen spezifiziert werden. Per *Änderungen speichern* wird die Anfrage verschickt. Der Status der Anfrage ist unter *Datenanfragen* für den Nutzer einsehbar.



Wenn die Löschanfrage bestätigt wird, wird der Nutzeraccount gesperrt und die Daten werden zum Löschen vorbereitet. Sofern Löschfristen für bestimmte Datenarten hinterlegt werden und dabei festgelegt wurde, dass die Daten bei Löschanfragen des Nutzers nicht gelöscht werden, bleiben diese Daten erhalten und werden erst nach Ablauf der Löschfrist zum Löschen vorbereitet.

3 Richtlinien/Einwilligungen verwalten

In diesem Abschnitt erfahren Sie, wie die Funktion zur Hinterlegung von Einwilligungen oder Nutzerinformationen erfolgt. Dieses Verfahren ersetzt den bisherigen Prozess durch Hinterlegung einer Datei. Mit dem neuen Verfahren ist die Verwaltung wesentlich vereinfacht und zugleich ein Berichtswesen erstellt worden.

3.1 Plugin aktivieren

Folgen Sie dem Pfad: *Website-Administration → Nutzer/innen → Datenschutz und Richtlinien→ Richtlinieneinstellungen*

Sie haben im Feld „Datenschutz der Website" nun zwei Optionen zur Auswahl:

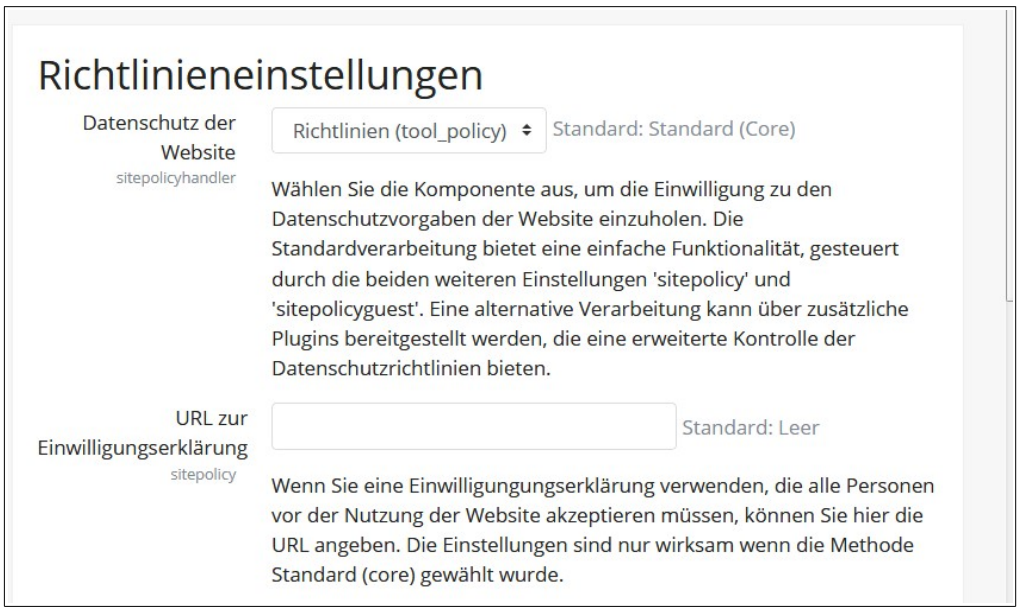
3.1.1 „Standard (Core)"

Bei der Auswahl dieser Option können Sie im Feld darunter („URL zur Einwilligungserklärung") den Link zu Ihrer Einwilligungserklärung einfügen. Nutzern der Website wird diese dann angezeigt. Hierbei handelt es sich um das ‚alte' Verfahren zur Hinterlegung von Datenschutzerklärungen. Die neuen Funktionen für Berichte und Versionsverwaltungen stehen nicht zur Verfügung.

Wir empfehlen dieses Verfahren nicht weiter zu nutzen.

3.1.2 „Richtlinien (tool_policy)"

Bei der Auswahl dieser Option kann die neue Funktion über das Plugin „Richtlinien (tool_policy)" genutzt werden, welches eine erweiterte Kontrolle der Datenschutzrichtlinien bietet. Erst nach Aktivierung der Funktion steht ein neuer Menüpunkt ‚Richtlinien verwalten' unter Datenschutz und Richtlinien zur Verfügung.



3.2 Neue Texte einpflegen/Versionen verwalten

Folgen Sie dem Pfad: *Website-Administration → Nutzer/innen → Datenschutz und Richtlinien → Richtlinien verwalten.*

Um einen neuen Text einzupflegen, klicken Sie nun auf „Neue Richtlinie".

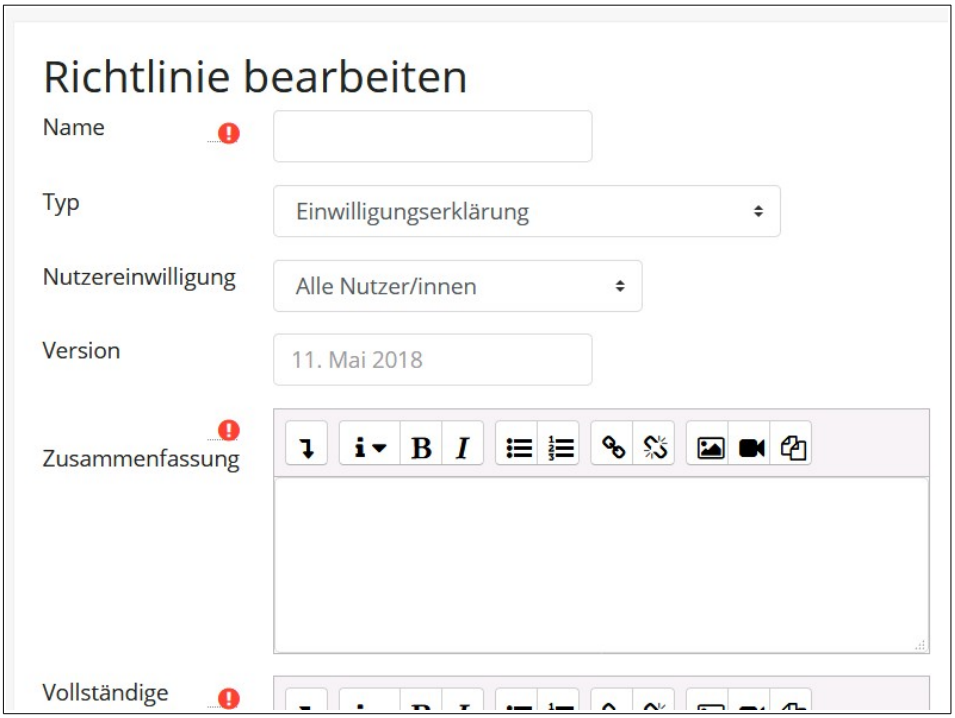
Es gibt die Möglichkeit, dass der gesamte Informationstext zu Datenschutz in einer einzelnen Richtlinie hinterlegt wird. Sie haben jedoch auch die Möglichkeit, mehrere Teilabschnitte als Einzelrichtlinien anzulegen. Ein Nutzer muss jeden einzelnen Teil der Richtlinie bestätigen, damit die Richtlinie insgesamt als bestätigt gilt.

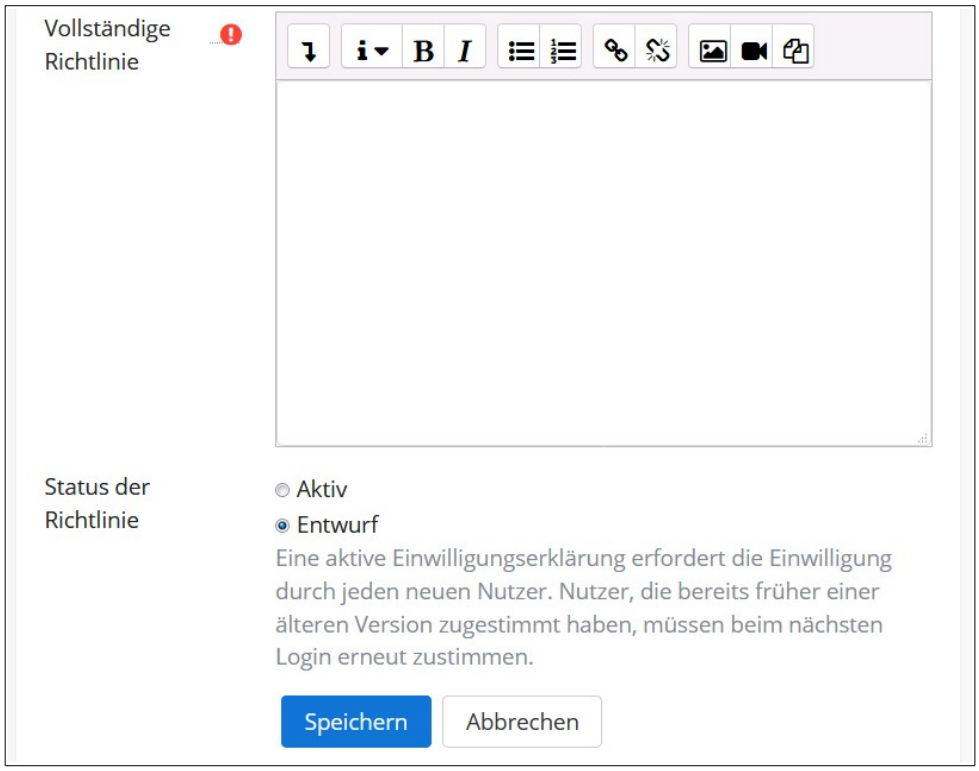
Die Aufteilung in mehrere Richtlinien schafft eine gute Übersicht. Zugleich kann es für einen Teilnehmer jedoch auch zur Herausforderung werden, mehrere Teilrichtlinien bestätigen zu müssen.

Dem Nutzer wird beim Zugriff erst jede einzelne Richtlinie auf einer separaten Seite angezeigt. Nach dem letzten Richtlinienteil werden auf einer Übersichtsseite nur die Zusammenfassungen angezeigt.

Richtlinienteile können erst als Entwurf erstellt werden. Wenn sie aktiviert werden, müssen Nutzer sie bestätigen. Es gibt die Möglichkeiten bereits aktivierte Richtlinienteile zu überarbeiten. Wenn Sie geringfügige Änderungen (z.B. Tippfehlerkorrekturen) vornehmen, kreuzen Sie das an. Diese Änderungen müssen nicht erneut bestätigt werden.

Ein Textteil, der als Entwurf gekennzeichnet ist, wird dem Nutzer noch nicht zur Einwilligung vorgelegt. Wenn ein Textteil aktiviert wird, müssen beim nächsten Login alle Nutzer die Einwilligung neu geben. Es ist daher sinnvoll, das Versionsfeld z.B. mit einem Datum oder einer fortlaufenden Nummer zu bezeichnen. Einmal aktivierte Richtlinien können nicht gelöscht werden.


Richtlinie bearbeiten
Name
Typ
Einwilligungserklärung
Nutzereinwilligung
Alle Nutzer/innen
Version
11. Mai 2018
Zusammenfassung
Vollständige


Vollständige Richtlinie
Status der Richtlinie
Aktiv
Entwurf
Eine aktive Einwilligungserklärung erfordert die Einwilligung durch jeden neuen Nutzer. Nutzer, die bereits früher einer älteren Version zugestimmt haben, müssen beim nächsten Login erneut zustimmen.
Speichern
Abbrechen

Name	Dies ist der Name, der Nutzern angezeigt wird. Er sollte daher möglichst präzise sein.
Typ	Wählen Sie den Typ des Textes aus: „Einwilligungserklärung" „Datenschutzregelung" „Regelungen zur Datenweitergabe an Dritte" „Andere Richtlinien" Der Richtlinientyp ist nur im Verwaltungsbereich „Richtlinien und Einwilligungen" sichtbar und wird Nutzern nicht angezeigt.
Nutzereinwilligung	Hier legen Sie fest, ob der Text allen Nutzern, nur authentifizierten Nutzern, oder Gästen zur Einwilligung vorgelegt wird.
Version	Hier springt automatisch das aktuelle Datum als Standard ein. Wenn mehrere Versionen an einem Tag erstellt wurden, steht dahinter jeweils ein Suffix „v1", „v2", „v3" usw. Sie können statt des Datums natürlich auch selbst einen beliebigen Wert, z.B. eine fortlaufende Nummer, an dieser Stelle eintragen.
Zusammenfassung	Tragen Sie hier eine Kurzbeschreibung der gesamten Richtlinie in klarer, verständlicher Sprache ein.
Vollständige Richtlinie	Fügen Sie hier den gesamten Text der Richtlinie ein. Achten Sie auch hier auf gut verständliche Sprache.
Status der Richtlinie	„Aktiv": Nutzer müssen der Richtlinie zustimmen „Entwurf": Die Richtlinie wird gespeichert, aber Nutzern noch nicht angezeigt.

3.3 Einen Text oder mehrere Teile erstellen?

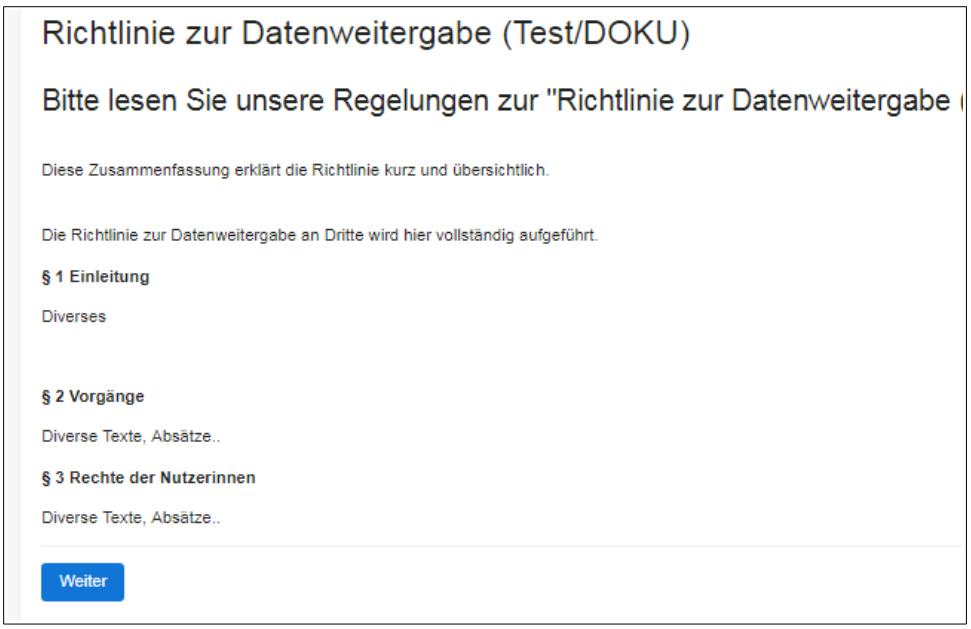
Die Einwilligung kann als ein geschlossener Text angelegt oder in mehrere Teile aufgeteilt werden. Der Nutzer wird erst jeden Teil auf einer einzelnen Seite sehen und kann von Abschnitt zu Abschnitt wechseln. Danach wird ihm auf einer Übersicht die Zusammenfassung für jeden einzelnen Teil angezeigt. Jeder Teil muss hier einzeln bestätigt werden. Nur wenn alle Teile bestätigt sind, gilt die Einwilligung als gegeben.

3.4 Texte später überarbeiten/Versionen verwalten

Um gespeicherte Richtlinien zu bearbeiten, erhalten Sie unter *Website-Administration → Nutzer/innen → Datenschutz und Richtlinien → Richtlinien verwalten* eine Übersicht über alle erstellten Richtlinien. Über das Schnellmenü *Aktionen* erreichen Sie die Option *Bearbeiten*. Klicken Sie diese an, können Sie Änderungen an den Texten, Namen oder Versionsnummern Ihrer Richtlinien vornehmen. Das Schnellmenü Aktionen erlaubt außerdem den Wechsel des aktuellen Status' der Richtlinie (Entwurf/Aktiv).

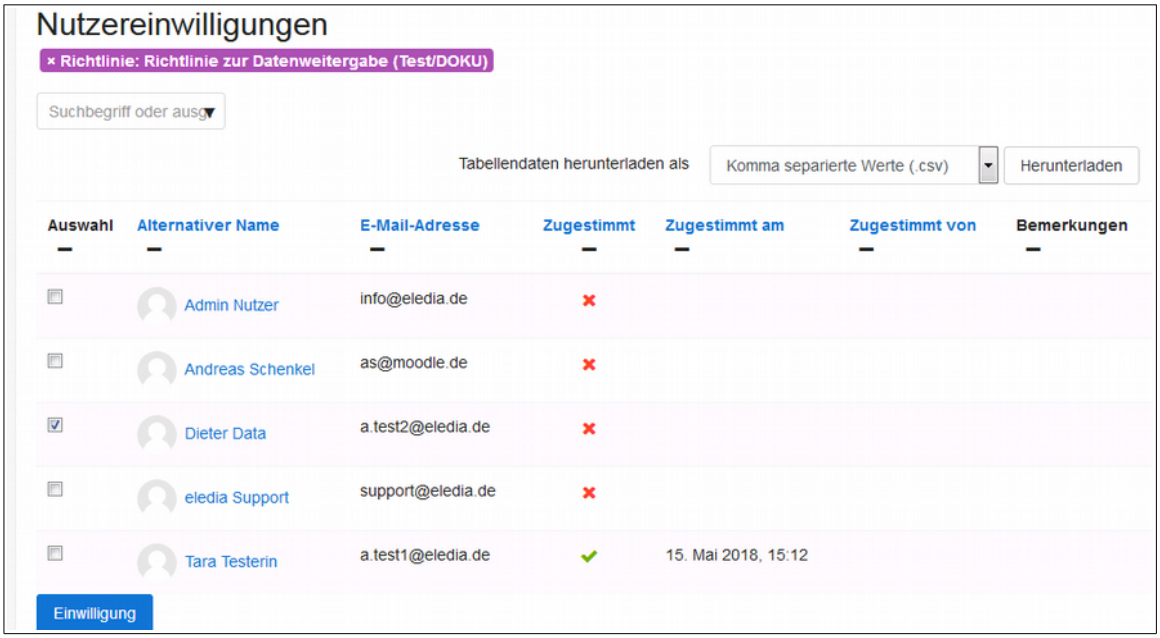
3.5 Im Namen anderer Nutzer Einwilligung hinterlegen

Sind Richtlinien für ein System aktiv, müssen Nutzer vor dem nächsten Login alle Richtlinienteile akzeptieren, bevor Sie zu Ihrem Nutzerprofil gelangen.

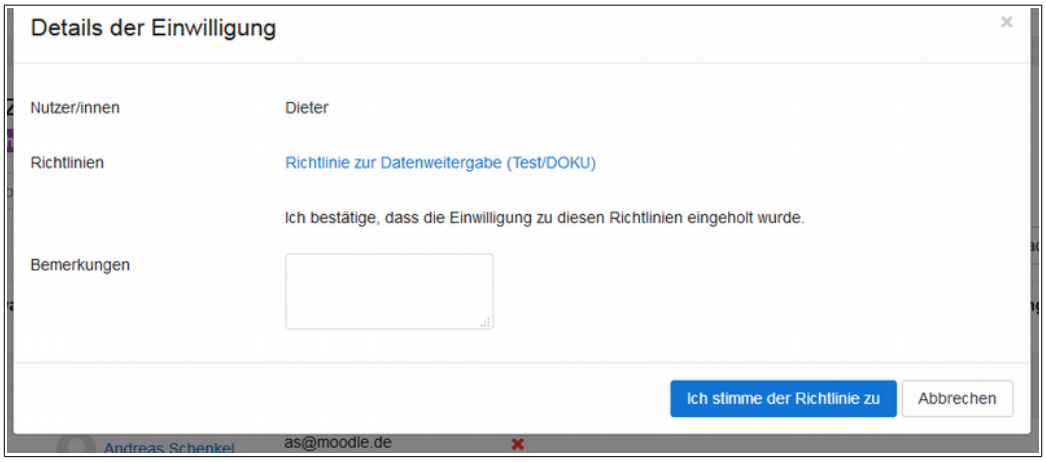


Unter *Website-Administration → Nutzer/innen→Datenschutz und Richtlinien → Nutzereinwilligungen* können durch den Admin oder einen entsprechend berechtigten Account Einwilligungen im Namen anderer Nutzer gegeben werden. Der entsprechende Nutzer wird dazu über die Checkbox markiert.

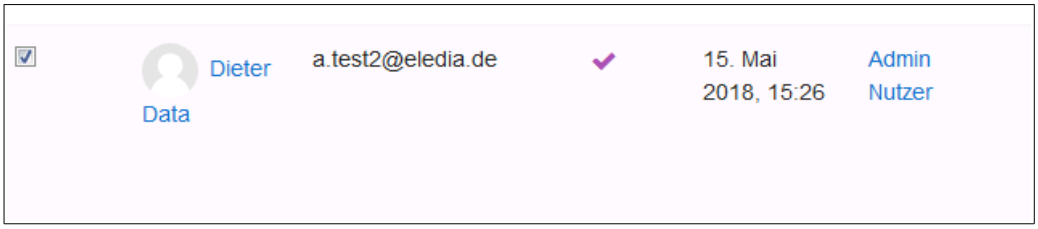
Dies ist sinnvoll, wenn die Information/Zustimmung auf anderem Weg erfolgt ist.



Über den Button *Einwilligung* öffnet sich ein neues Fenster, in dem im Namen dieses Nutzers die Zustimmung zu einer Richtlinie erteilt werden kann. Eine Einwilligung, die beispielsweise der Admin für einen anderen Nutzer vornimmt, ist in der Übersicht der Nutzereinwilligungen entsprechend markiert. Der Haken für die Einwilligung ist nicht grün, wie bei einer Einwilligung durch den Nutzer, sondern lila.

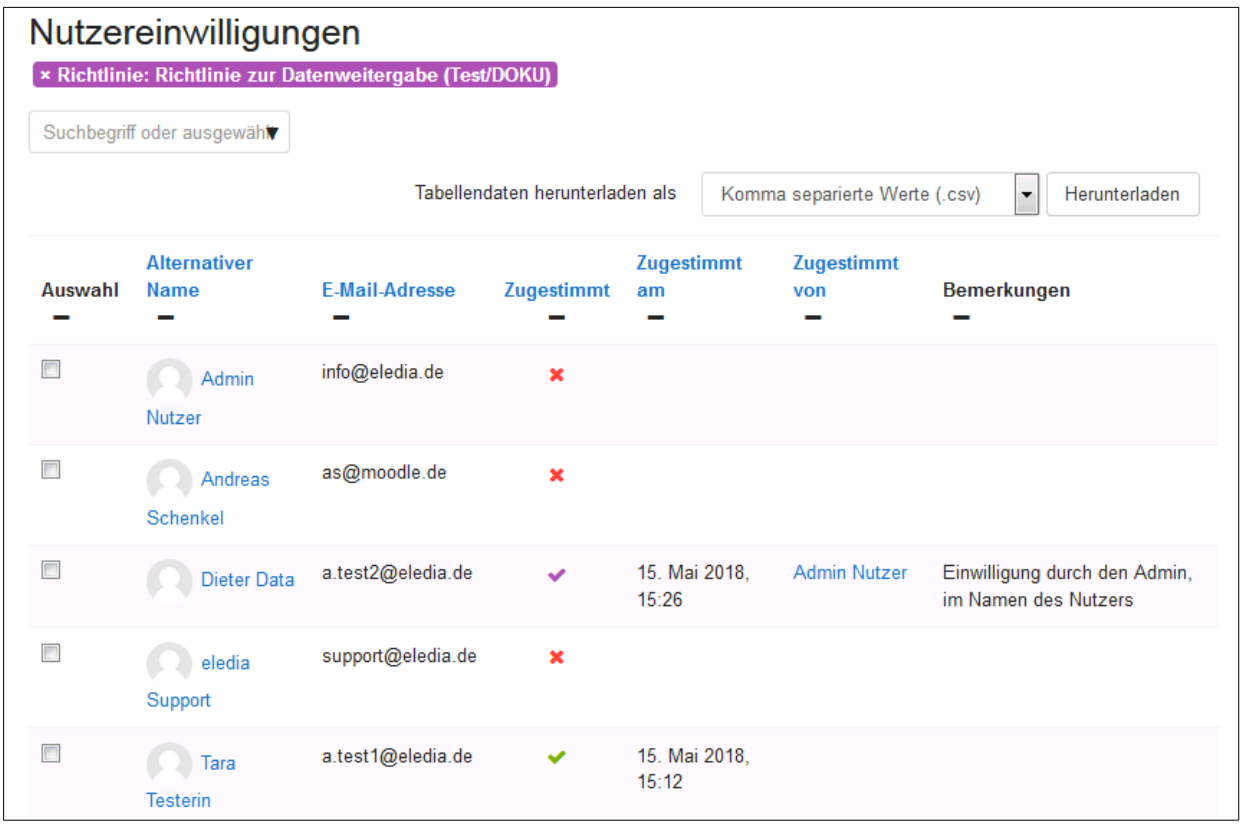


Durch die Bemerkung kann der Grund für die Information/Einwilligung durch eine andere Person dokumentiert werden.



3.6 Berichte einsehen

Aktive Richtlinien lassen sich unter *Website-Administration → Nutzer/innen → Datenschutz und Richtlinien → Nutzereinwilligungen* beobachten und bearbeiten. Der Admin oder Datenschutzansprechpartner erhält hier eine Übersicht über alle Nutzer und über den Stand der Zustimmungen zu einer Richtlinie. Er kann hier auch im Namen von Nutzern einer Richtlinie zustimmen (s.o.). Neben einer Such- und Filterfunktion für verschiedene Nutzer oder Richtlinien lassen sich Tabellendaten exportieren.

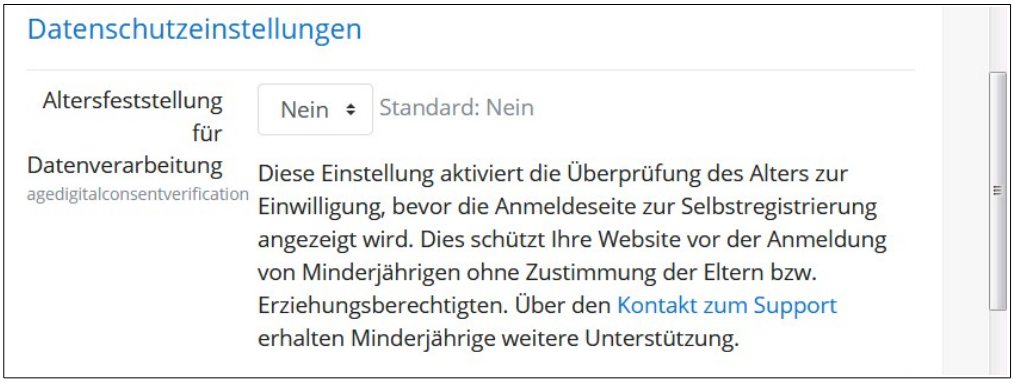


4 Altersgrenze bei der Nutzerselbstregistrierung

Sie können eine Altersgrenze für bei der Nutzerselbstregistrierung festlegen. Wichtig: Diese Funktion wird nur genutzt, wenn Nutzer berechtigt sind, ihre Accounts selber anzulegen.

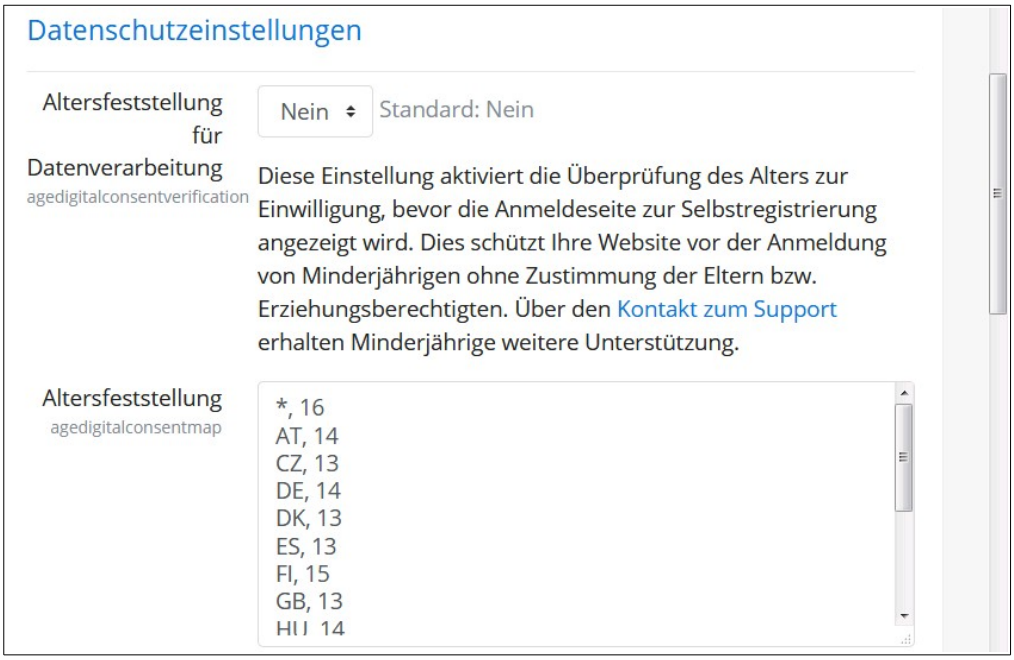
Folgen Sie dazu dem Pfad: *Website-Administration → Nutzer/innen → Datenschutz und Richtlinien → Datenschutzeinstellungen*

Um die Funktion zu aktivieren, wählen Sie für das Feld „Altersfeststellung für Datenverarbeitung" die Option „Ja" aus.



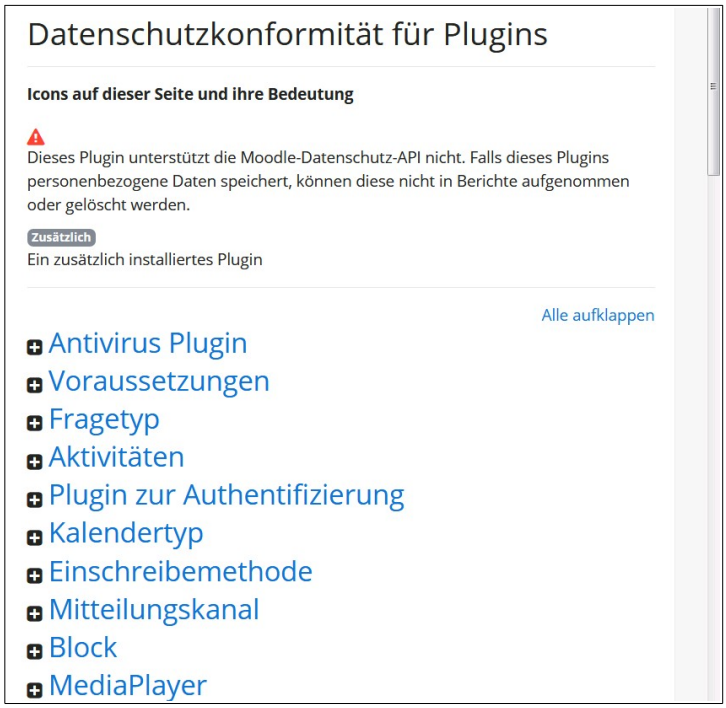
Ist diese Option aktiviert, müssen Nutzer bei einer Selbstregistrierung zunächst ihr Alter und ihr Herkunftsland eingeben, bevor sie zur Registrierungsseite gelangen. Der Nutzer wählt dazu das Land aus und bestätigt, dass das Alter über dem für dieses Land definierten digitalen Einwilligungsalter liegt. Ist der Nutzer unter diesem Alter, erscheint der Hinweis, dass eine erziehungsberechtigte Person den Support der Seite kontaktieren kann.

Im Feld *Altersfeststellung* kann das standardmäßige digitale Einwilligungsalter angegeben werden. Außerdem lässt sich ein abweichendes Einwilligungsalter für einzelne Länder hinterlegen. Geben Sie dazu jedes Alter in einer neuen Zeile mit folgendem Format ein: Ländercode, Alter (getrennt durch ein Komma). Das Standardalter wird durch * anstelle des Ländercodes angezeigt. Die derzeitige Liste entspricht dem aktuellen Stand der nationalen Gesetzgebung.



5 Übersicht über die Verwaltung personenbezogener Daten in den Plugins

Moodle ist in vielen einzelnen Elementen strukturiert. Diese Plugins haben häufig eigene Tabellen in der Datenbank. In vielen dieser Tabellen werden auch personenbezogene Daten gespeichert. Die Übersicht zeigt, von welchen Plugins persönliche Daten der Nutzer gespeichert werden. Sie erreichen die Übersicht über *Website-Administration → Nutzer/innen→ Datenschutz und Richtlinien → Datenschutzübersicht für Plugins.*



Die Standardplugins von Moodle sind so angepasst worden, dass die von Ihnen angelegten persönlichen Daten bei einem Wunsch auf einen Bericht über gespeicherte Daten aufgenommen werden. Bei einem Löschantrag müssen die entsprechenden Einträge gelöscht werden.

Wenn bei Ihnen zusätzliche Plugins installiert sind, können auch diese personenbezogene Daten speichern. Die Entwickler dieser Plugins müssen Anpassungen vornehmen, damit die Datenbankeinträge gelöscht werden können.

Wenn für ein Plugin die Anpassungen noch nicht erfolgt sind, warnt Moodle in der Übersicht. Die Warnung erkennen Sie an einem roten Achtung-Icon. In der aufgeklappten Plugin-Liste wird zudem ersichtlich, wenn es sich um ein zusätzlich installiertes Plugin handelt.

6 Verwaltung der Datenlöschprozesse

Moodle kennt verschiedene Möglichkeiten, Daten zu löschen. Beim Löschen einer Lernaktivität oder eines Kurses werden zugleich alle damit verbundenen persönlichen Nutzerdaten gelöscht. Wenn ein Nutzer, der in einen Kurs eingeschrieben ist, aus dem Kurs ausgetragen wird, ist damit das Löschen seiner persönlichen Daten im Kurs nicht verknüpft. Würde der Nutzer später wieder in den Kurs eingeschrieben, könnte er bei seinem früheren Bearbeitungsstand das Lernen fortsetzen.

Wenn ein Nutzeraccount in der Nutzerverwaltung gelöscht wird, sind keine Daten von ihm mehr sichtbar. Der Nutzeraccount kann nicht wieder hergestellt werden.

Mit den neuen datenschutzrechtlichen Plugins werden erweiterte Löschverfahren und -prozesse eingeführt. Sie enthalten - vereinfacht gesagt - folgende Funktionen:

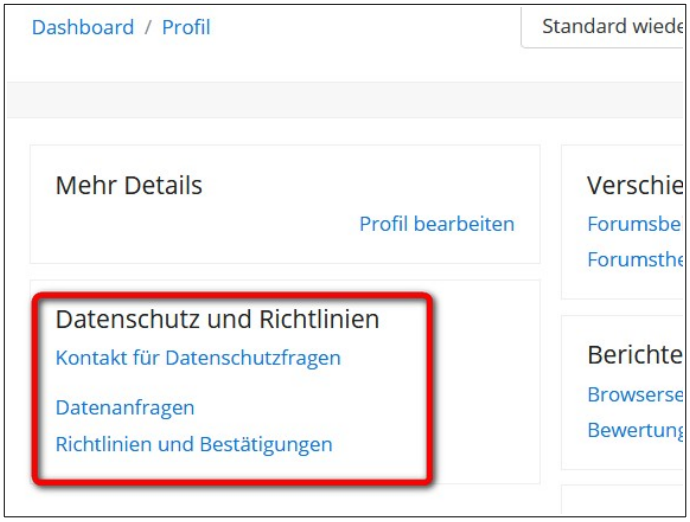
- Ein Nutzer kann beantragen, dass seine persönlichen Daten gelöscht werden. Dieser Wunsch muss manuell bestätigt werden bevor er ausgeführt wird.
- Für Kurse kann festgelegt werden, dass die darin enthaltenen personenbezogenen Daten nach Ablauf einer Frist nach Kursende gelöscht werden. Der Löschvorgang wird auch hier manuell gestartet. Kursinhalte werden nicht gelöscht.
- Wenn es institutionelle Kriterien zur Aufbewahrung von Daten (z.B. Kursabschlüsse, Tests, Aufgabenlösungen) gibt, kann festgelegt werden, dass diese bei einem Löschwunsch des Nutzers nicht gelöscht werden.

Datenschutzrechtlich ist der Löschwunsch eines Nutzers nicht absolut gesetzt. Wenn im Unternehmen z.B. Nachweise über durchgeführte Schulungen gefordert sind oder Prüfungsnachweise im Studium aufbewahrt werden müssen, hat der Plattformbetreiber ein berechtigtes Interesse, die Daten weiter zu speichern. In einzelnen Fällen kann dies durch Vertrag, Prüfungsordnung, interne oder gesetzliche Regelungen begründet sein.

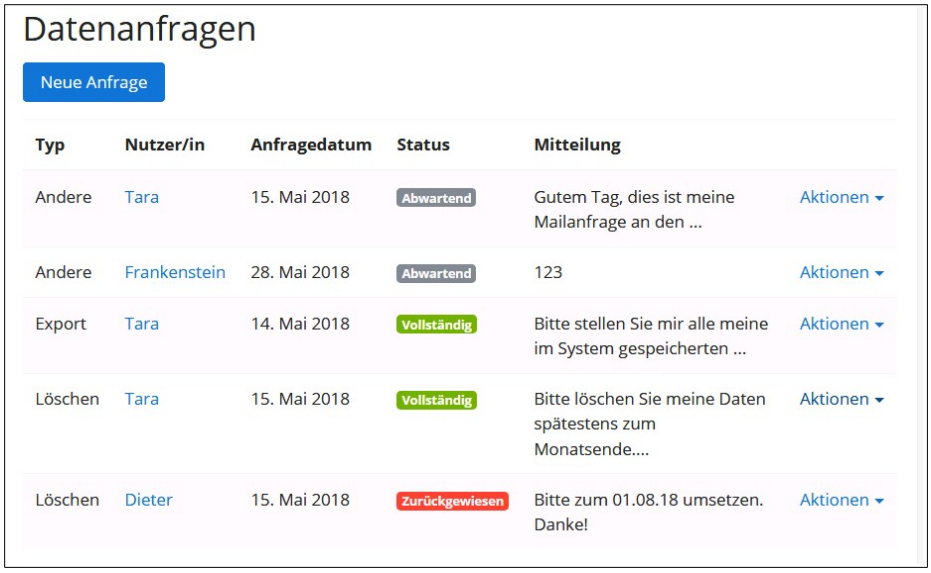
Wichtig ist: alle Formen derartiger Löschungen erfolgen nicht automatisch. Sie werden vorbereitet und manuell angestoßen.

6.1 Löschanträge der Nutzer

Jeder Nutzer kann in seinem Profil im Abschnitt ‚Datenschutz und Richtlinien' unter ‚Datenanfragen' den Wunsch äußern, dass seine Daten gelöscht werden. Dies löst eine Benachrichtigung an die zuständigen Personen in Moodle aus.



Unter Datenanfragen finden diese eine Liste aller Anfragen. In der ersten Spalte wird der Typ der Datenfrage angezeigt. In der letzten Spalte besteht die Möglichkeit, die Anfrage zu bestätigen.

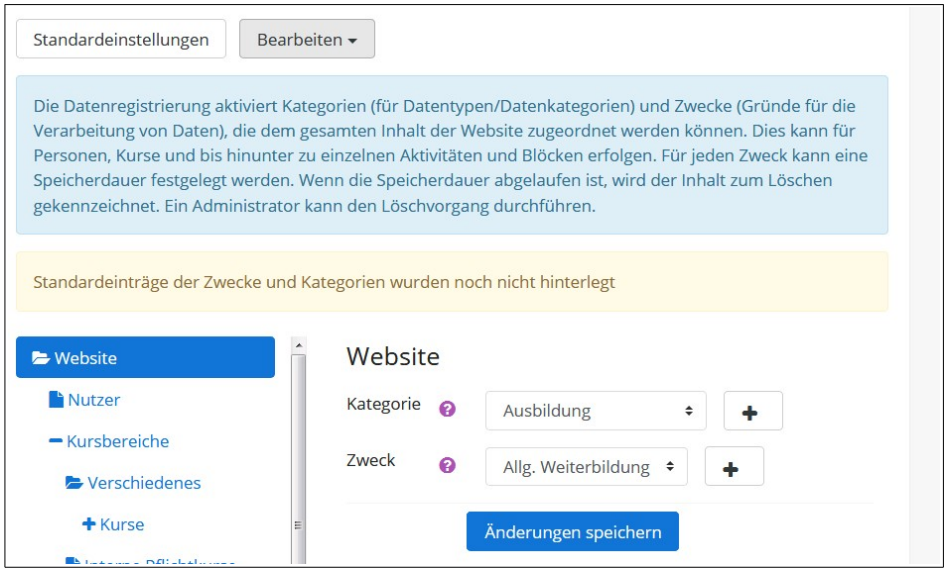


Mit der Bestätigung einer Löschanfrage des Nutzers werden in allen Kursen personenbezogene Daten des Nutzers gelöscht, sofern sie nicht auf ‚geschützt' gesetzt wurden. Zugleich wird der Nutzeraccount gelöscht. Ein weiterer Zugriff des Nutzers auf das System ist nicht möglich.

Der Nutzer kann nicht beantragen, dass nur Daten eines bestimmten Kurses gelöscht werden.

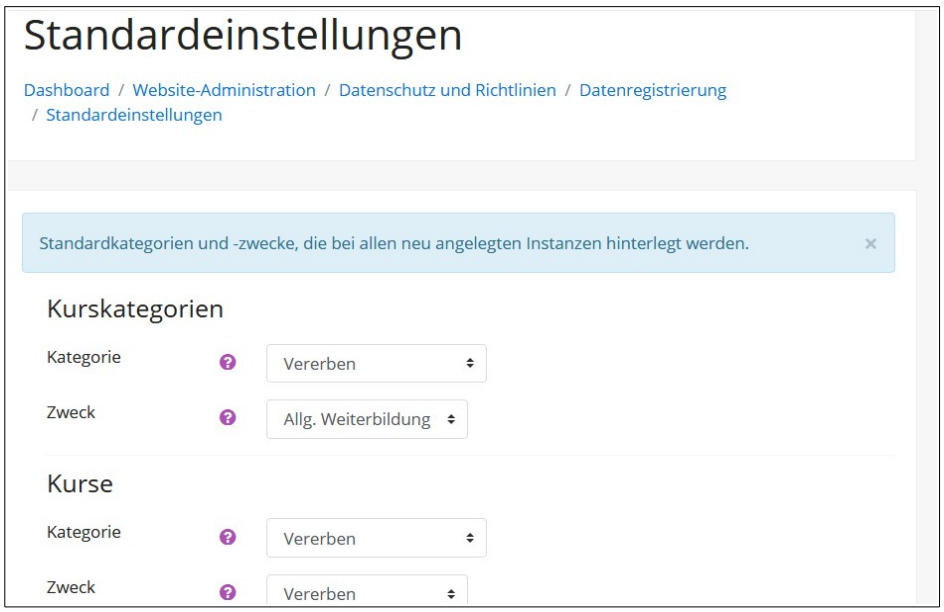
6.2 Festlegung der Löschfristen für Kurse

Unter Website-Adminstration → Nutzer/innen → Datenschutz und Richtlinien → Datenregistrierung können Sie alle Informationen über die Kategorien verarbeiteter Daten, den Zweck der Verarbeitung, Standardlöschfristen und Löschsperren festlegen.

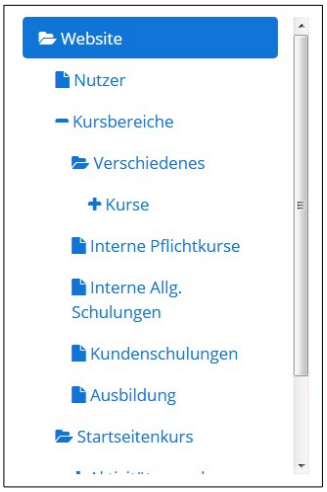


Unter ‚Bearbeiten' können Sie zunächst verschiedene Kategorien von Daten hinterlegen und Zwecke der Verarbeitung definieren. Im Formular für die Zwecke befinden sich Einstellungen für Standardlöschfristen und die ‚Löschschutzsperre'.

Dann haben Sie die Möglichkeit unter Standardeinstellungen für Kurskategorien, Kurse, Aktivitätsmodule und Blöcke Standardwerte festzulegen. Diese werden als Standardwert auf alle Ebenen ‚nach unten' vererbt.



Der Navigationsbaum bildet das gesamte Moodle-System ab. Diesen kann man aufrufen, um an einer beliebigen Stelle einen vom Standard abweichenden Eintrag vorzunehmen. Es ist daher sinnvoll, zunächst den allgemeinen Wert zu setzen, der fast überall verwendet werden soll, und danach Ausnahmen anzulegen.



Ein Beispiel:

Typischerweise sollen personenbezogen Daten in allen Kursen vier Wochen nach Kursende gelöscht werden. Setzen Sie dies als Standardwert.

Sie haben jedoch eine Kurskategorie für die betrieblichen Pflichtkurse. Diese Daten dürfen erst nach drei Jahren gelöscht werden. Legen Sie dazu eine zweite Kategorie von Datenverarbeitungen ‚Pflichtkurse' an und weisen Sie sie der Kurskategorie ‚Pflichtkurse' zu.

6.2.1 Anlegen von Kategorien

Bei Kategorien von Daten geht es um eine grobe Beschreibung, welche Art von Daten in einem bestimmten Bereich verarbeitet werden. Die Daten helfen bei der Dokumentation. Einträge könnten z.B.

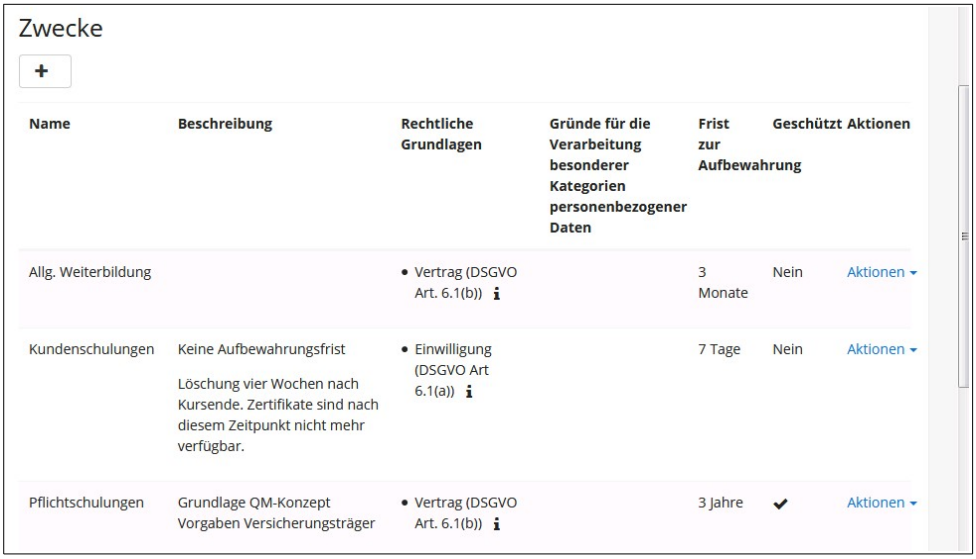
sein: Kurskommunikation, Prüfungsergebnisse.

Klicken Sie auf ‚Bearbeiten' und ‚Kategorien', um eine neue Datenkategorie anzulegen. Über das +-Symbol legen Sie eine neue Kategorie an.

Das Formular enthält nur zwei Felder für den Namen und eine Beschreibung.

6.2.2 Anlegen von Zwecken der Verarbeitung

Unter ‚Bearbeiten' ‚Zwecke' kann in gleicher Weise ein Formular aufgerufen werden, das jedoch umfassender ist.

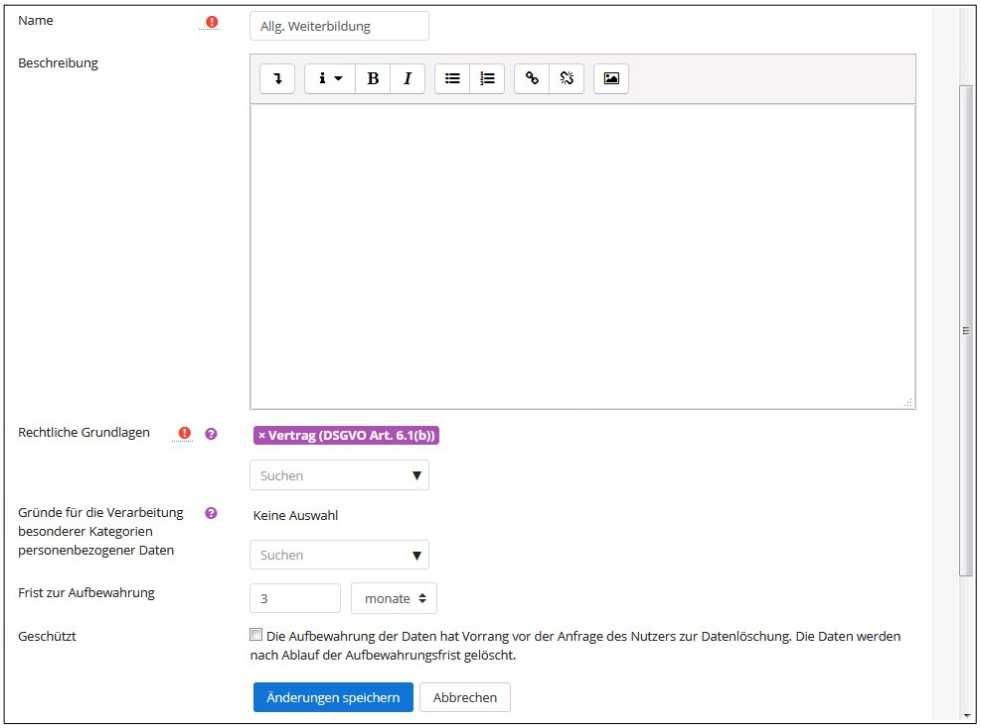


Name und Beschreibung sind selbsterklärend. Die nächsten beiden Felder ermöglichen es anzugeben, auf welchen rechtlichen Grundlagen die Verarbeitung erfolgt. Die Auswahloptionen entsprechen den in der Datenschutzgrundverordnung genannten Grundlagen. Es können nacheinander mehrere Grundlagen ausgewählt werden.

Die Datenschutzgrundverordnung kennt ‚besondere Kategorien personenbezogener Daten'. Diese Daten sind besonders schützenswert. Diese können im zweiten Auswahlbereich hinterlegt werden. Im Bildungsbereich werden diese aber sehr selten zum Einsatz kommen.

Der Eintrag zur Aufbewahrungsfrist ermöglicht Ihnen, festzulegen, wann die personenbezogenen Daten in einem Kurs gelöscht werden. Bezugspunkt für die Berechnung ist immer das Kursendedatum in den Einstellungen eines Kurses.

Wichtiger Hinweis: Wenn in einem Kurs kein Kursendedatum gesetzt ist, werden in diesem Kurs keine personenbezogenen Daten gelöscht.



Die Festlegungen können in Jahren, Monaten oder Tagen vorgenommen werden.

Wenn Sie das Häkchen für ‚Geschützt' setzen, wird verhindert, dass diese Daten bei einem individuellen Löschantrag eines Nutzers gelöscht werden. In dem Fall erfolgt die Löschung der Daten erst mit dem Löschen der Daten im Kurs.

6.3 Festlegung von Sperren für das Löschen von Nutzerdaten

Bei der Festlegung jedes einzelnen Zwecks können Sie das Häkchen für ‚geschützt' setzen. Dies bewirkt, dass die personenbezogenen Daten bei einem individuellen Löschantrag nicht gelöscht werden. Die Daten werden erst mit dem ‚regulären' Löschprozess entfernt.

Die Löschsperren können in unterschiedlichen Situationen wichtig sein. Einige Beispiele:

- gesetzliche Aufbewahrungspflichten für prüfungsrelevante Leistungen und Informationen,
- Nachweise über Schulungen für betriebliche Audits,
- Nachweis vertraglich erbrachter Leistungen z.B. im Rahmen von Rechtsstreitigkeiten mit dem Nutzer,
- weitere Nutzung des Kurses durch andere Teilnehmer. Damit kann ich z.B. das Löschen von Forenbeiträgen eines Nutzers abweisen.

Im Normalfall denkt man beim Löschen an die persönlichen Daten eines Teilnehmers. Daten, die von einem Trainer oder Prüfer erfasst werden, sind jedoch auch dessen personenbezogene Daten. Wenn nun ein Trainer einen Löschwunsch hat, wie soll damit umgegangen werden? Diese Situation ist tatsächlich schwierig. Es gibt inzwischen Rechtsprechung, die die Bewertung und den Kommentar zu einer Aufgabe durch einen Trainer zu einem personenbezogen Datum des Teilnehmers erklärt, der bewertet wurde. Im Grunde ist damit die Bewertung ein personenbezogenes Datum beider Personen. Eine Löschung darf dann nur vorgenommen werden, wenn beide Personen einen Löschantrag stellen oder die Aufbewahrungspflicht abgelaufen ist. Praktisch sollte in solchen Fällen nur die Löschung nach Ende der Aufbewahrungsfrist zur Anwendung kommen.

6.4 Bestätigung des Löschens von personenbezogenen Daten in Kursen

Unter *Website-Administration → Nutzer/innen → Datenschutz und Richtlinien → Datenlöschung* wird eine Liste von Kursen erstellt, in denen personenbezogene Daten gelöscht werden können. Kurse oder Kursinhalte werden dort aufgelistet, wenn nach Kursendedatum die Speicherfrist abgelaufen ist. Sie können die Elemente markieren, die gelöscht werden sollen.

Die Löschung wird dann angestoßen und nach und nach ausgeführt. Da im Einzelfall sehr viele Daten an verschiedenen Stellen zu löschen sind, wird dies nicht sofort, sondern im Hintergrund ausgeführt.