Technische und organisatorische Maßnahmen beim Auftragnehmer Oehl.Net GmbH

Die **Anforderungen an die Sicherheit der Datenverarbeitung § 64 BDSG (neu)**

bilden für uns die Grundlage beim Umgang mit personenbezogene Daten. Die Benutzung der Lernplattform bietet den Anbietenden und Teilnehmenden konkreter Lehrveranstaltungen die Möglichkeit der kurs- und personenbezogenen Kommunikation zum Zwecke der Organisation des Unterrichts und Gruppenarbeiten sowie zum Austausch von Lehrmaterial und schriftlichen Studienleistungen. Die Speicherung der genannten Daten ist notwendig, um sicherzustellen, dass relevante Informationen kommuniziert werden und eine angemessene Bewertung der so erbrachten Studienleistungen durchgeführt werden kann.

Die interne Verarbeitung personenbezogener Daten ist so gestaltet, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei werden Maßnahmen getroffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind.

dazu **bietet § 64 BDSG-neu** eine Übersicht (vgl. https://dsgvo-gesetz.de/bdsg-neu/64-bdsg-neu/):

§ 64 BDSG (neu)Anforderungen an die Sicherheit der Datenverarbeitung und Umsetzung bei der Oehl.Net GmbH

1. Der Verantwortliche und der Auftragsverarbeiter haben unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um bei der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten. Der Verantwortliche hat hierbei die einschlägigen Technischen Richtlinien und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik zu berücksichtigen.

2. Die in Absatz 1 genannten Maßnahmen können unter anderem die Pseudonymisierung und Verschlüsselung personenbezogener Daten umfassen, soweit solche Mittel in Anbetracht der Verarbeitungszwecke möglich sind. Die Maßnahmen nach Absatz 1 sollen dazu führen, dass

    1. die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt werden und

    2. die Verfügbarkeit der personenbezogenen Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.

3. Im Fall einer automatisierten Verarbeitung haben der Verantwortliche und der Auftragsverarbeiter nach einer Risikobewertung Maßnahmen zu ergreifen, die Folgendes bezwecken:

    1. **Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (Zugangskontrolle),**

       Das Hosting der Plattform erfolgt durch die Strato AG. Details siehe ‚Vereinbarung zur Auftragsverarbeitung Oehl.Net mit Strato 20180516.pdf'

       Datenbestände werden mit Zugriffspasswörtern geschützt. Den Serverzugriff haben nur ausgewählte und zum Datenschutz verpflichtete Personen.
       Die verwendeten Server verfügen über Firewalls und Virenscanner, kritische Datenübertragungen im Internet erfolgen mit SSL-Verschlüsselung.

    2. **Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern (Datenträgerkontrolle),**

       Datenbestände werden mit Zugriffspasswörtern geschützt. Den Serverzugriff haben nur ausgewählte und zum Datenschutz verpflichtete Personen.
       Die verwendeten Server verfügen über Firewalls und Virenscanner, kritische Datenübertragungen im Internet erfolgen mit SSL-Verschlüsselung.

    3. **Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (Speicherkontrolle),**

       Der zugrundeliegende Webanwendungsserver verfügt über ein Sicherheits-Framework, das auf sogenannten Rollen (englisch Roles) aufbaut und genaue Festlegungen erlaubt, wer wo was darf. Für jedes einzelne Objekt kann festgelegt werden, welche Rolle für welche Art des Zugriffs benötigt wird; diese Rollen können den einzelnen Benutzern auch lokal zugewiesen werden, um ihnen z. B. Zugriff nur in einem bestimmten Teilbaum zu gewähren.
       Darüber hinaus arbeitet der Web-Benutzer nicht wie bei klassischen Skriptsprachen (wie PHP, Perl u. ä.) im Dateisystem des Servers, sondern in einer gesonderten virtuellen Umgebung. Aus dieser auszubrechen ist nur möglich, wenn es vom Entwickler gewünscht wird. Dieses System verhindert Zugriffe auf andere auf dem Server gespeicherte Informationen und unterläuft damit gängige Angriffsmuster.
       Die verwendeten Server verfügen über Firewalls und Virenscanner, kritische Datenübertragungen im Internet erfolgen mit SSL-

Verschlüsselung.

4. **Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (Benutzerkontrolle),**

   Die verwendeten Server verfügen über Firewalls und Virenscanner, kritische Datenübertragungen im Internet erfolgen mit SSL-Verschlüsselung. Während des Studiums mit der Lern- und Wissensplattform angelegte Bezüge des Accounts zu noch existierenden Objekten sind erst nach der Löschung anonymisiert. Die Speicherung erfolgt in einer Weise, dass die Daten gegen einen unberechtigten Zugriff Dritter geschützt sind.

5. **Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben (Zugriffskontrolle),**

   Der Seitenzugriff wird über einen rollenbasierten Rechteparser gesteuert. Er stellt kritische Informationen nur ausgewählten und entsprechend zum Datenschutz verpflichteten Personen zur Verfügung.

6. **Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle),**

   Die Weitergabe von personenbezogene Daten erfolgt nur in einem klar definierten Rahmen. Ein mit dem Auftraggeber abgestimmtes Reportingmodell liefert dabei ausgewählten personalverantwortlichen Mitarbeitern seitens des Auftraggebers für die Durchführung der Schulungsmaßnahmen erforderliche Informationen zum Lernfortschritt der Lerner. In zukünftigen Systemversionen werden auch ausgewählte Tutoren den Lernfortschritt explizit zugeordneter Lerner erhalten (zur Unterstützung von Peer-Tutoring).

   Das Reporting ist passwortgeschützt. Der Zugriff ist nur für Personen mit entsprechend erweiterten Rechten möglich. Vor Freigabe werden die Personen unterrichtet bezüglich ihrer Verpflichtung zur Einhaltung der datenschutzrechtlichen Anforderungen nach der DSGVO. Marktmanager erhalten Zugriff auf im Markt beschäftigte Mitarbeiter, Tutoren auf ihre Lerngruppe und Personalentwickler auf alle Mitarbeiter der Baumarktkette.

7. **Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit**

und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind (Eingabekontrolle),

Eingaben werden mit Benutzername und Datum registriert und protokolliert.

8. **Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden (Transportkontrolle),**

   Datenübertragungen im Internet erfolgen mit SSL-Verschlüsselung.

9. **Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (Wiederherstellbarkeit),**

   Die Daten werden täglich gesichert.

10. **Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit),**

    Die personalverantwortlichen Mitarbeiter und Lernende beim Auftraggeber und die Mitarbeiter der Oehl.Net GmbH arbeiten intensiv mit der bereitgestellten Plattform. Störungen werden unverzüglich gemeldet und zeitnah behoben.

11. **Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität),**

    Fehlfunktionen können nicht vollständig ausgeschlossen werden aber durch verantwortliche Programmierung und permanente Optimierung und Korrektur minimiert. Die Daten werden täglich gesichert.

    Das Hosting der Plattform erfolgt durch die Strato AG. Details siehe ‚Vereinbarung zur Auftragsverarbeitung Oehl.Net mit Strato 20180516.pdf‘

12. **Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),**

    Hierzu gibt es klare Vereinbarungen (z.B. Löschung nicht bestandener Prüfungen werden i.d.R. von den Personalverantwortlichen (Personalentwicklung, Marktmanager, Tutor) angefordert.

    Wenn entsprechend vereinbart können aber auch die Lerner selbst solche Löschungen anfordern. Details zu diesen Verfahren werden in

der Praxis per Email kommuniziert und für die Verantwortlichen transparent umgesetzt. Dabei wird versucht, die Interessen aller Beteiligten zu wahren, aber auch den administrativen Aufwand begrenzt zu halten.

13. **Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),**

    Die Daten werden täglich gesichert.

14. **Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können (Trennbarkeit).**

    Der Seitenzugriff wird über einen rollenbasierten Rechteparser gesteuert. Er stellt kritische Informationen nur ausgewählten und entsprechend zum Datenschutz verpflichteten Personen zur Verfügung.

Ein Zweck nach Satz 1 Nummer 2 bis 5 kann insbesondere durch die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren erreicht werden.