



Improved Reading GmbH & Co. KG

**Datenschutz-Konzept
Für die Webcoached Plattform**

Teil 1

Konkrete Angaben zur Auftragsverarbeitung

Gemäß Art. 28 Abs. 3 Datenschutz–Grundverordnung (DS-GVO) :

1. Gegenstand des Auftrages

Webcoached ist eine Plattform der Improved Reading GmbH & Co. KG. Sie verarbeitet personenbezogene Daten im Auftrag seiner Auftraggeber. Gegenstand des Auftrags ist die Durchführung von webbasierten Weiterbildungsmaßnahmen für die Mitarbeiterinnen und Mitarbeiter des Auftraggebers über die Webcoached-Plattform.

2. Dauer des Auftrages

Die Dauer dieses Auftrags (Laufzeit) wird mit dem Auftraggeber individuell vereinbart.

3. Art und Zweck der Verarbeitung von Daten

- a) Zweck der Verarbeitung:
Durchführung von webbasierten Weiterbildungsmaßnahmen für die Mitarbeiterinnen und Mitarbeiter des Auftraggebers
- b) Art der Verarbeitung (Beschreibung der einzelnen Verarbeitungsschritte)
Zur Erfüllung seiner Aufgaben und Erbringung seiner Leistungen führt Webcoached folgende Arbeitsschritte durch:
 - Übernahme der von Kursteilnehmern eingegebener Daten zwecks Zusendung von Zugangsdaten zum System.
 - Nutzung der Daten innerhalb des E-Learning-Systems zum Zwecke der systeminternen Kommunikation zwischen Dozent und Teilnehmer.
 - Erstellung eines Zertifikats nach Abschluss der Maßnahme.

4. Art der Daten

Im Zusammenhang mit der vorbeschriebenen Leistungserbringung werden vom Webcoached folgende Datenarten/ -kategorien verarbeitet:

- Vorname
- Nachname
- E-Mail-Adresse
- Während der Maßnahme erzielte Übungsergebnisse

5. Kategorien der betroffenen Personen

Die Kategorien der Personen, die durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags betroffen sind, umfassen:

- Mitarbeiterinnen und Mitarbeiter des Auftraggebers

6. Ansprechpartner für Fragen des Datenschutzes:

peter.stonn@webcoached.de, Geschäftsführer, 02161-4688178

Teil 2

Allgemeine Regelungen zur Auftragsverarbeitung

Allgemeine Bestimmungen

- (1) Der Auftraggeber ist als „Verantwortlicher“ i.S.d. Art. 4 Nr. 7 Datenschutz-Grundverordnung (DS-GVO) für die Einhaltung der Vorschriften über den Datenschutz, für die Rechtmäßigkeit der Datenverarbeitung i.S.d. Art. 4 Nr. 2 DS-GVO, insbesondere der Datenweitergabe an Webcoached, sowie für die Wahrnehmung der Rechte der Betroffenen verantwortlich. Webcoached unterstützt den Auftraggeber hierbei in geeigneter Weise. Darüber hinaus verpflichtet sich Webcoached zur Einhaltung sämtlicher einschlägiger datenschutzrechtlicher Vorschriften im Rahmen der Ausführung des Auftrages.
- (2) Bei der E-Mail-Kommunikation achten Auftraggeber und Webcoached auf die Vertraulichkeit, indem sie vertrauliche Informationen gegen unberechtigte Kenntnisnahme oder Manipulationen schützen. Hierzu können die Parteien entsprechende technische Maßnahmen, z.B. Verschlüsselungs- und Signaturverfahren, abstimmen.
- (3) Webcoached bestätigt und stellt sicher, dass die für die Durchführung des Auftrags eingesetzten Personen zur Vertraulichkeit verpflichtet sind und in die Schutzbestimmungen der DS-GVO eingewiesen worden sind.
- (4) Etwaige Datenschutzverstöße werden von Webcoached unverzüglich gemeldet.
- (5) Soweit Webcoached ihre Leistung in den Räumlichkeiten oder unter Zugriff auf die Systeme des Auftraggebers erbringt, unterliegt er den Kontrolleinrichtungen des Auftraggebers (insbesondere Zutritts-, Zugangs- und Zugriffskontrolle).
- (6) Webcoached kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
- (7) Webcoached unterstützt den Auftraggeber bei der Einhaltung der DS-GVO zur Sicherheit personenbezogener Daten, bei Meldepflichten bei Datenpannen, ggf. bei einer Datenschutz-Folgeabschätzungen und vorherige Konsultationen und insbesondere zur Erfüllung der Rechte der betroffenen Person gemäß Art. 12 – 23 DS-GVO.
- (8) Datenschutzrechtliche Auskünfte an Dritte oder den Betroffenen erteilt Webcoached nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber.

Ort der Datenverarbeitung

- (1) Die Verarbeitung der Daten erfolgt ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR). Falls die Anwendung der DS-GVO in den Staaten des EWR nicht verbindlich beschlossen wurde, gelten die Staaten des EWR als Drittländer.
- (2) Jede Verlagerung in ein Drittland erfolgt ausschließlich bei Zustimmung des Auftraggebers und nur, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

Unverzüglich Meldungen und Informationspflichten bei Datenschutzverletzungen

- (1) Webcoached informiert den Auftraggeber bei Unregelmäßigkeiten des Datenverarbeitungsablaufes, bei begründetem Verdacht der Verletzung von Vorschriften und Vereinbarungen zum Schutz personenbezogener Daten. Webcoached sichert zu, den Auftraggeber bei möglichen Informationspflichten nach Artikel 33 – 34 DS-GVO zu unterstützen.
- (2) Die Meldung an den Auftraggeber erfolgt unverzüglich, nachdem Webcoached die Verletzung bekannt wurde.
- (3) Jede Datenschutzverletzung wird von Webcoached dokumentiert. Die Dokumentation und Meldung einer Datenschutzverletzung enthält mindestens folgende Informationen:
 1. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
 2. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
 3. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
 4. eine Beschreibung der von Webcoached ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.Darüber erteilt Webcoached dem Auftraggeber alle sonstigen Informationen, die der Auftraggeber für die Erfüllung seiner eigenen Meldepflichten benötigt.

Subunternehmer

- (1) Sollte es für die konkrete Auftragsdurchführung erforderlich sein, Subunternehmer einzusetzen, wird dies zwischen Webcoached und dem Auftraggeber pro Einzelfall vereinbart.
- (2) Webcoached verpflichtet in dem Fall seine Subunternehmer auf die Einhaltung datenschutzrechtlicher Vorschriften sowie etwaiger zusätzlicher Vereinbarungen mit dem Auftraggeber.

Berichtigung und Löschung von Daten

- (1) Webcoached berichtigt oder löscht die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Aufforderung durch den Auftraggeber.
- (2) Der Auftraggeber kann vorbehaltlich gesetzlicher Aufbewahrungspflichten oder sonstiger entgegenstehender Rechtsvorschriften auch während der Laufzeit und nach Beendigung des Vertrages jederzeit die Berichtigung, Löschung, Sperrung (i.S.d. Einschränkung der Verarbeitung gem. Art. 4 Nr. 3 DS-GVO) und Herausgabe von personenbezogenen Daten verlangen.

§ 7 Technische und organisatorische Sicherheitsmaßnahmen nach Art.32 DS-GVO

- (1) Webcoached gestaltet seine Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei werden insbesondere Maßnahmen getroffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind.
- (2) Webcoached beachtet die Grundsätze für die Verarbeitung personenbezogener Daten aus Art. 5 Abs. 1, Abs. 2 DS-GVO und gewährleistet die vertraglich vereinbarten und gesetzlich erforderlichen Datensicherheitsmaßnahmen gem. Art. 24, Art. 28, Art. 32 DS-GVO, um den Nachweis zu erbringen, dass die Verarbeitung gemäß der DS-GVO erfolgt.
- (3) Webcoached vergibt Zugriffsberechtigungen nur an Personen, die mit der Durchführung des Auftrags befasst sind. Auf Verlangen kann Webcoached dem Auftraggeber die zugriffsberechtigten Personen und deren Berechtigungen benennen.
- (4) Webcoached spielt keine personenbezogene Daten in Systeme Dritter. Dies gilt auch für Testzwecke.
- (5) Webcoached verwendet während der Entwicklung von Software oder der Prüfung und Wartung automatisierter Verfahren fiktive Testdaten oder nach ausdrücklicher schriftlicher Einwilligung durch den Auftraggeber anonymisierte Originaldaten.
- (6) Die vereinbarten Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung und werden von Webcoached dem aktuellen Stand der Technik angepasst. Dies gilt ebenso im Fall von Anordnungen der zuständigen Aufsichtsbehörden. Wesentliche Änderungen (z.B. wesentliche Änderung von Verschlüsselungsverfahren oder Anmeldeprozeduren) werden dokumentiert.
- (7) Webcoached gewährleistet die ordnungsgemäße Durchführung der technischen und organisatorischen Maßnahmen (Teil 3 der DuD-B, „TOM“).

Teil 3

Technische und organisatorische Maßnahmen (TOM)

Webcoached trifft geeignete technische und organisatorische Maßnahmen (Art. 32 DS-GVO), um ein dem Risiko angemessenes Schutzniveau im Hinblick auf die erforderliche Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer zu gewährleisten.

Diese Maßnahmen schließen folgendes ein:

Der Server wird in Deutschland am Sitz der Hetzner Online AG in 91710 Gunzenhausen gehostet.

Die verteilten Rechenzentren von Hetzner sind groß und als solche von außen nicht erkennbar. Die genaue Wegbeschreibung wird nur auf Anfrage bekannt gegeben.

Zugangs- und Zutrittskontrolle:

Die Ein- und Ausgänge des Servers sind kameragesteuert.

Der Zugang ist nur seinen Vertragspartnern mit Terminvereinbarung und Identitätsnachweis gestattet. Bevollmächtigte Vertreter bedürfen der schriftlichen Bestätigung des Vertragspartners.

Der Zugang zu den Serverräumen ist nur in Begleitung eines Mitarbeiters möglich.

Sicherheit:

Die unterbrechungsfreie Stromversorgung wird durch eine Batteriekapazität von 15 Minuten und durch Notstromdiesel gewährleistet.

Die Klimatisierung erfolgt über ein Doppelbodensystem.

Eine moderne Brandmeldeanlage ist direkt an die Brandmeldezentrale der örtlichen Feuerwehr angeschlossen. Wenn das System einen Fehler feststellt, wird das Sicherheitsunternehmen automatisch informiert.

Die Hetzner-Rechenzentren befinden sich in Deutschland (Falkenstein und Nürnberg), einem Land im Rahmen der GDPR-Vorschriften.

Auf den Servern von CPD2, die sich im Besitz von Hetzner (Falkenstein) befinden, wird eine Remote-Sicherheitskopie erstellt, die den Bestimmungen des Organgesetzes 15/1999 entspricht.

Der Zugriff auf die Server ist auf das technische Personal der PIXELXEN S.L. und der Webcoached GmbH & Co. KG, insbesondere Herrn Esteve Rodríguez beschränkt.

Der direkte Zugriff auf die Server ist nur über die IP von PIXELXEN S.L. und einigen anderen Servern von PIXELXEN S.L. (Backup, Monitoring und Management) sowie von der Webcoached GmbH & Co. KG möglich.

Die Zugangspasswörter wurden geändert, als PIXELXEN S.L. die Administration des Systems übernahm und dem Verantwortlichen der Webcoached GmbH & Co. KG zur Verfügung gestellt.

Auch die SSH-Schlüssel wurden für alle Benutzer außer den von der Webcoached GmbH & Co. KG ersetzt.

Folgende Mitglieder des PIXELXEN S.L. Teams haben Root-Zugriff auf den Server:

- Fernando Méndez
- Forlidar Macías
- Iñaki Olazabal
- José Luis Arroyo
- Miguel Sánchez

Betriebssystem

Das Betriebssystem des Servers ist Debian 7.11.

Dateiübertragungs-Richtlinie

Die aktuelle Richtlinie zur Übertragung nicht öffentlicher Dateien auf und von Servern verhindert den Zugriff über unverschlüsselte Protokolle wie FTP / webdav.

Updates

Alle Sicherheitsupdates des Debian-Betriebssystems werden wöchentlich überprüft und alle zwei Monate aktualisiert.

Monitoring

Das zentrale Überwachungssystem basiert auf einer in Deutschland ansässigen CPD, die keine direkte Kommunikation mit den für die Erbringung der vertraglichen Leistungen verwendeten CPDs hat.

Das Monitoring-System ist für die Überwachung des Status von Diensten zuständig. Der Status wird alle 5 Minuten abgefragt, um die Antwortzeit für alle öffentlichen Dienste zu erhalten und um den Status der Maschine/Server zu erhalten, wodurch Administratoren über mögliche Fehlfunktionen im System informiert werden.

Fehlertoleranz-System

Die gesamte Hardware, die dem Dienst des genannten Servers zugeordnet ist, ist redundant: Duale Stromversorgung, RAID-Festplatte.

PixelXen S.L. weist SLAs auf, die den vertraglich vereinbarten Leistungen entsprechen.

Nur das Personal der CPDs, die die von PixelXen S.L. beauftragten Server hosten, hat physischen Zugriff auf die Server.

Mönchengladbach, Mai 2020

Improved Reading GmbH & Co. KG