Vertrag zur Auftragsverarbeitung (AV-Vertrag)

Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag
i.S. d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO)

zwischen dem Kunden

_____

_____

- Verantwortlicher - nachstehend „Auftraggeber“ genannt –

und der

InterMedia Solutions GmbH, Ahornstr. 7, 82041 Oberhaching

- Auftragsverarbeiter - nachstehend „Auftragnehmer“ genannt

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Gegenstand der Vereinbarung sind die Rechte und Pflichten der Parteien im Rahmen der Leistungserbringung gemäß Auftrag, Leistungsbeschreibung und AGB, soweit eine Verarbeitung von personenbezogenen Daten durch den Auftragnehmer als Auftragsverarbeiter für den Auftraggeber gemäß Art. 28 DSGVO erfolgt.

Dies umfasst alle Tätigkeiten, die der Auftragnehmer zur Erfüllung des Auftrags erbringt und die eine Auftragsverarbeitung darstellen. Dies gilt auch, sofern der Auftrag nicht ausdrücklich auf diese Vereinbarung zur Auftragsverarbeitung verweist.

(2) Dauer

Die Dauer der Verarbeitung entspricht der im Auftrag vereinbarten Laufzeit.

2. Art und Zweck der Verarbeitung

(1) Die Art der Verarbeitung umfasst alle Arten von Verarbeitungen im Sinne der DSGVO zur Erfüllung des Auftrags.

(2) Art der verarbeiteten, personenbezogenen Daten bestimmt der Auftraggeber durch die Produktwahl, die Konfiguration, die Nutzung der Dienste und die Übermittlung von Daten.

(3) Die Kategorien von Betroffenen bei der Verarbeitung personenbezogenen Daten bestimmt der Auftraggeber durch die Produktwahl, die Konfiguration, die Nutzung der Dienste und die Übermittlung von Daten. Die Verarbeitung senibler, personenbezogenen Daten gemäß Art. 9 DSGVO wird ausgeschlossen.

(3) Zwecke der Verarbeitung sind alle zur Erbringung der vertraglich vereinbarten Leistung im Bereich Cloud-Dienstleistungen, Hosting, Software as a Service (SaaS) und IT-Support erforderlichen Zwecke.

3. Technisch-organisatorische Maßnahmen

Einzelheiten zu den technischen und organisatorischen Maßnahmen befinden sich in der Anlage.

(1) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen.

(2) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Verantwortlichkeit und Verarbeitung (Berichtigung, Einschränkung und Löschung von Daten)

(1) Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Best-immungen der Datenschutzgesetze, insbesondere für die Recht¬mäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwort-licher« im Sinne des Art. 4 Nr. 7 DSGVO). Dies gilt auch im Hinblick auf die in dieser Vereinbarung geregelten Zwecke und Mittel der Verarbeitung.

(2) Die Weisungen werden anfänglich durch den Auftrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) durch einzelne Weisungen geändert werden (Einzelweisung). Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen. Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Bei Änderungsvorschlägen teilt der Auftragnehmer dem Auftraggeber mit, welche Auswirkungen sich auf die vereinbarten Leistungen, insbesondere die Möglichkeit der Leistungserbringung, Termine und Vergütung ergeben. Ist dem Auftragnehmer die Umsetzung der Weisung nicht zumutbar, so ist der Auftragnehmer berechtigt, die Verarbeitung zu beenden. Eine Un-zumutbarkeit liegt insbesondere vor, wenn die Leistungen in einer Infrastruktur erbracht werden, die von mehreren Auftraggebern / Kunden des Auftragnehmers genutzt wird (Shared Services), und eine Änderung der Verarbeitung für einzelne Auftraggeber nicht möglich oder nicht zumutbar ist.

(3) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(4) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

(5) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird:
Herr Robert Holzer, Tel. 089-244 150 51,
datenschutz@intermedia-solutions.de
benannt.
b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO.
d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
g) Der Auftragnehmer 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.

h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Auftragsverarbeiter im Sinne des Art. 28 DSGVO zur Vertragserfüllung einzusetzen.

(3) Die aktuell eingesetzten weiteren Auftragsverarbeiter sind nachstehend aufgeführt. Der Auftraggeber erklärt sich mit deren Einsatz einverstanden.

- 1&1 Internet SE, Elgendorfer Str. 57, 56410 Montabaur
- TenshiTec, Neustift 7, 85622 Weißenfeld

(4) Der Auftragnehmer informiert den Auftraggeber, wenn er eine Änderung in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter beabsichtigt. Der Auftraggeber kann gegen derartige Änderungen Einspruch erheben.

(5) Der Einspruch gegen die beabsichtigte Änderung kann nur aus einem wichtigen datenschutz-rechtlichen Grund innerhalb einer angemessenen Frist nach Zugang der Information über die Änderung gegenüber dem Auftragnehmer erhoben werden. Im Fall des Einspruchs kann der Auftragnehmer nach eigener Wahl die Leistung ohne die beabsichtigte Änderung erbringen oder - sofern die Erbringung der Leistung ohne die beabsichtigte Änderung für den Auftragnehmer nicht zumutbar ist - die von der Änderung betroffene Leistung gegenüber dem Auftraggeber innerhalb einer angemessenen Frist nach Zugang des Einspruchs einstellen.

(6) Erteilt der Auftragnehmer Aufträge an weitere Auftragsverarbeiter, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag auf den weiteren Auftragsverarbeiter zu übertragen.

(7) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, erfolgt durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist

berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

11. Vertragslaufzeit, Sonstiges

(1) Die Vereinbarung beginnt mit dem Abschluss durch den Kunden. Sie endet mit Ende des letzten Vertrages unter der o.g. Kundennummer. Sollte eine Auftragsverarbeitung noch nach Beendigung dieses Vertrages stattfinden, gelten die Regelungen dieser Vereinbarungen bis zum tatsächli-chen Ende der Verarbeitung.

(2) Der Auftragnehmer kann die Vereinbarung nach billigem Ermessen mit angemessener Ankündigungsfrist ändern.

(3) Ergänzend gelten die AGB des Auftragnehmers, abrufbar unter https://www.intermedia-solutions.net/pdf/agb.pdf. Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung zur Auftragsverarbeitung den Regelungen des Hauptvertrages vor. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarungen im Übrigen nicht.

(4) Ausschließlicher Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit diesem Vertrag ist München. Dieser gilt vorbehaltlich eines etwaigen ausschließlich gesetzlichen Gerichtsstandes. Dieser Vertrag unterliegt den gesetzlichen Bestimmungen der Bundesrepublik Deutschland.

(5) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und

das Eigentum an den Daten ausschließlich beim Auftraggeber als „Verantwortlicher“ im Sinne der DSGVO liegen.

Oberhaching, den _____

_____
Robert Holzer, Geschäftsführer
„Auftragnehmer“

_____
Ort, Datum

_____
Name, Titel
„Auftraggeber“

Anlage: Technisch-organisatorische Maßnahmen

Anlage
Technisch-organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Zutrittskontrolle
  Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen;
- Zugangskontrolle
  Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
- Zugriffskontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- Weitergabekontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Verfügbarkeitskontrolle
  Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Datenschutz-Management;
- Incident-Response-Management;
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);
- Auftragskontrolle
  Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

InterMedia Solutions
IMS a complete webcasting suite

Verarbeitungsverzeichnis

gemäß Art 30 DSGVO

Inhaltsverzeichnis

Auftragsdatenverarbeiter

InterMedia Solutions GmbH
(nachstehend IMS genannt)
Ahornstr. 7, 82041 Oberhaching bei München

Ansprechpartner: Robert Holzer
Tel: +49 89-244 151 51
E-Mail: datenschutz@intermedia-solutions.de

Produktbeschreibung – IMS Webcast Plattform

IMS entwickelt und betreibt eine webbasierte Streaming- und Webcast Plattform, deren Grundfunktion die Veröffentlichung von Live Video Streams und On Demand Video Aufzeichnungen über das Internet ist. Zum Betrieb werden die folgenden Systemen genutzt.

IMS Streaming & Hosting Services:
Ein Cloud Servernetzwerk ermöglicht die Speicherung sowie hoch performante Auslieferung von Streaming Video und Web- / Download Content.

IMS Webcast CMS:
Das CMS (Content Management System) ermöglicht es eine eigene Webseite bzw. Webseiten zur Veröffentlichung und Steuerung von Videos und Livestreams zu erstellen. Mit zusätzlichen Funktionalitäten kann die Webseite individuell gestaltet, der Zugang geschützt und um interaktive Module erweitert werden.

Die Veröffentlichung erfolgt über einen Link der das Webcast Projekt in einem Browser öffnet, bzw. über bestehende Webseiten auf denen es eingebunden ist.

Nutzer & Rechte

Es gibt grundsätzlich nur einen (Haupt) Zugang zum Kundenkonto. Innerhalb des Kundenkontos können (optional) weiter (Teil) Zugänge angelegt werden.

Kunde/Eigentümer (Administrator)	Hat vollen Zugriff auf alle Funktionalitäten und kann (optional) Passwort geschützte (Teil) Zugänge, für nachfolgende Bereiche und Funktionalitäten, erstellen.
IMS (Optional)	Gemäß Kundenauftrag IMS kann vom Kunden zum Setup und Support beauftragt werden.
Eventmanager (Optional)	Teilnehmerverwaltung Teilnehmer/daten anlegen, bearbeiten, exportieren, löschen
Eventmanager (Optional)	Umfrageverwaltung Umfragen anlegen, anzeigen, bearbeiten, auswerten, exportieren, löschen

Moderator (optional)	Nachrichtenverwaltung Eingehende Nachrichten sichten, sortieren, priorisieren, exportieren, löschen
Eventmanager (Optional)	Web RTC Webmeetings anlegen, moderieren, löschen

Einladungsmanagement / Registrierung

IMS unterstützt folgende Einladungsvarianten:

- Teilnehmer können per E-Mail eingeladen werden. Weitere Möglichkeiten sind auch ein Link auf einer öffentlichen bzw. internen Website, Social Networks, Foren, oder Intranet-Applikationen.
- Datentransfer per csv/xls Datei
  Teilnehmerdaten können in das System importiert werden.
- Selbstregistrierung
  Datenfelder sind in beliebiger Anzahl frei definierbar, optional können Pflichtfelder definiert werden sowie reine Textfelder oder Felder zur freien Texteingabe.
- Passwortoptionen
  Passwort wird automatisiert vom System vergeben oder vom Kunden/Eigentümer vordefiniert.
- Login mit individualisiertem Benutzernamen und Passwort

Teilnehmerverwaltung / Datennutzung

Die Abfrage und Speicherung von Teilnehmerdaten in einer zentralen Datenbank ist optional möglich.

Folgende Webcast Module benötigen, den Zugriff auf die Nutzerdatenbank, bzw. ermöglichen eine Nutzung und Veröffentlichung von Teilnehmerdaten:

- Login / Registration
  Zugangsdaten werden mit den gespeicherten Teilnehmerdaten abgeglichen um den Zugang auf geschützte Seiten des Webcast Projektes zu ermöglichen.

- Message Box und Message Box Zuseher (Nachrichten versenden und anzeigen)
  Vom Teilnehmer versendete Nachrichten können (optional) mit den Teilnehmerdaten, im Backend (Admin Bereich) angezeigt werden. Zusätzlich ist es möglich Teilnehmerdaten, innerhalb der Webcast Oberfläche (für andere Teilnehmer sichtbar), zusammen mit der gesendeten Nachricht anzuzeigen.

- Umfragen / Tests:
  Umfrage- oder Testergebnisse können (optional) dem Teilnehmer zugeordnet werden.

- Teilnahme- und Teilnehmer Tracking:
  Das Nutzungsverhalten (Zeit und Dauer der Nutzung) (optional) dem Teilnehmer zugeordnet werden.

- IMS Web RTC – (Webmeeting):

Teilnehmerdaten können (optional) zur Anmeldung an der Webmeeting Funktionalität genutzt, sowie innerhalb eines Webmeetings (für andere Teilnehmer sichtbar) angezeigt.

Die Wahrung der Betroffenenrechte liegt in den genannte Fällen ausschließlich beim Kunden/ Eigentümer, da das System selbstständig keinerlei Teilnehmerdaten zuordnet, speichert oder veröffentlicht.

Aufzeichnungen

Die IMS Streaming & Hosting Services bieten die Möglichkeit Live Streams aufzuzeichnen, diese zu bearbeiten und als VOD (Video on Demand) zu veröffentlichen. Der Live Stream sowie die Aufzeichnung kann Personen sowie Personen aus dem Hintergrund erfassen.

Die Wahrung der Betroffenenrechte liegt in diesem Fall ausschließlich beim Kunden/ Eigentümer, da das System selbstständig keinerlei Live Streams oder Aufzeichnungen produziert.

Löschkonzept

Bei Löschung eines Webcast Projektes werden sämtliche damit in Verbindung stehenden Teilnehmer- und Projektdaten unwiderruflich gelöscht. Der Löschvorgang wird manuell durch einen berechtigten Nutzer initiiert.

Gewährleistung von Betroffenenrechten

IMS gewährt betroffenen Personen gem. Kapitel III DS-GVO das Recht auf Auskunft, Berichtigung, Löschung bzw. Sperrung, Datenübertragbarkeit und Widerruf. Sofern einer Löschung gesetzliche, vertragliche oder handels- bzw. steuerrechtliche Aufbewahrungsfristen oder sonstige gesetzlich Gründe entgegenstehen, werden die Daten nicht gelöscht, sondern mit einer Sperre versehen.
Zur Ausübung der vorgenannten Rechte können sich Betroffene wenden an:

InterMedia Solutions GmbH
Ahornstr. 7, 82041 Oberhaching bei München

Tel: +49 89-244 151 51
E-Mail: datenschutz@intermedia-solutions.de

Anwendungen und Systeme

Die Plattform besteht aus folgenden Systemen:

- Web- und Download Servern,
- Streaming-Server Cloud,

Hosting, Dienste und Streaming Systeme

IMS nutzt folgende Service Partner:

- Mircosoft Azure, Cloud Services,
- Ionos by 1und1, Serversysteme,

Die Bearbeitung, Verwaltung und Speicherung der Daten liegt in der Verantwortung von IMS. Der Betrieb der Hardware und Bereitstellung der datenverarbeitenden Infrastruktur liegt bei genannten Service Partnern und wird ausschließlich innerhalb der EU und gemäß GDPR (General Data Protection Regulation) bereitgestellt.

Zertifizierungen

Die Mircosoft Azure, Cloud Services haben unter anderem folgende Zertifizierungen erhalten:

- ISO 27001
- ISO 27018
- FedRAM
- FERPA
- HIPAA/HITECH
- SOC 1 und SOC 2 Typ 2-Berichte

Die Ionos by 1und1, Serversysteme, haben unter anderem folgende Zertifizierungen erhalten:

- ISO 9001
- ISO 27001
- PCI DSS

Sicherheitsmaßnahmen

Die zum Einsatz kommenden technischen und organisatorischen Maßnahmen werden im Folgenden beschrieben.

Vertraulichkeit – Zutritt

Regulierter physischer Zutritt zu Datenverarbeitungszentren
Die Zutrittskontrolle zu den Serverräumen wird durch die räumliche Struktur der jeweiligen Rechenzentren und dessen Betreiber gewährleistet.

Zugang - Regulierung des digitalen Zugangs zu IT

Systemen / Anwendungen

- Verschlüsselte Datenübertragung (SSL/SSH)
- Passwortgeschützter Systemzugang
- Rollenbasierte Zugriffskontrolle

- Multi-Factor Authentication (MFA)
- Protokollierung der Systemnutzung

Zugriff - Zugang zu Informationen

- Strikte Regelung und Einhaltung eines Zugriffsschema in der Anwendung
- Verhinderung von Unbefugten Lesen oder Manipulierens von Anwendungsdaten
- Zugriffserteilung auf “Need to know” Basis

Datentrennung

Personenbezogene Daten dürfen nur für den Zweck genutzt werden, für den sie ursprünglich erhoben wurden. Dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können, wird gewährleistet durch:

- Softwareseitigen Ausschluss (Mandantentrennung; Multitenancy-Architektur, rollenbasierte
- Zugriffskontrolle)
- Das Prinzip des geringsten Privilegs
- Das Datenbankprinzip, Trennung über Zugriffsregelung
- Trennung von Test- und Produktionsdaten
- Trennung von Entwicklungs- und Produktionsprogrammen

Integrität

Weitergabe - Verbot von unbefugtem Lesen von Daten bei der Übermittlung

- Abhörsichere Übertragung der Daten (SSL/SSH)
- Firewalls
- Virenschutz

Eingabe - Nachvollziehbarkeit der Quelle der Daten

Ob und von wem Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind, kann nachträglich überprüft und festgestellt werden durch:

- Benutzeridentifikation
- Protokollierung eingegebener Daten (Verarbeitungsprotokoll).

Verfügbarkeit und Belastbarkeit

Verfügbarkeit - Sicherheit gegen Verlust oder zufällige Zerstörung von Daten und Wiederherstellbarkeit

- Hosting in N+1 Konfigurationen
- Einsatz von RAID-Systemen
- Regelmäßige automatisierte Erstellung von Backups
- Zusätzliche manuelle Backup-Möglichkeit
- Mehrfache, getrennte Ablage der Backup-Daten

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Datenschutzfreundliche Voreinstellungen
- Regelmäßige, mindestens jährliche Prüfung und Überarbeitung der Maßnahmen

Auftragsdatenverarbeitung

Es ist sichergestellt, dass beauftragte externe Dienstleister die übertragenden personenbezogenen Daten mit gleicher Sorgfalt, dem Zweck entsprechend, verarbeiten.

Peer-to-Peer Enterprise CDN
Das Peer-to-Peer ECDN basiert auf nativen Browser-Features, d.h. die Konnektivität zwischen Peers und die damit verbundenen Sicherheitsaspekte sind Teil der Browser-Implementierung (WebRTCPeer-to-Peer-Verbindungen).

Es handelt sich um eine native Plattformkomponente von IMS, d.h. es sind keine zusätzlichen Datenprozessoren erforderlich. Die Verbindungen sind auf das lokale Netzwerk beschränkt und führen daher keine Netzwerkbrücken ein. Sie unterliegen netzwerk- und clientseitigen Firewall-Regeln.

Peer-to-Peer Enterprise CDN

Das Peer-to-Peer ECDN basiert auf nativen Browser-Features, d.h. die Konnektivität zwischen Peers und die damit verbundenen Sicherheitsaspekte sind Teil der Browser-Implementierung (WebRTCPeer-to-Peer-Verbindungen).
Es handelt sich um eine native Plattformkomponente von IMS, d.h. es sind keine zusätzlichen Datenprozessoren erforderlich. Die Verbindungen sind auf das lokale Netzwerk beschränkt und führen daher keine Netzwerkbrücken ein. Sie unterliegen netzwerk- und clientseitigen Firewall-Regeln.

Anlage: Externe Dienstleister

Microsoft Ireland Operations Ltd. South County Business Park, One Microsoft Place, Carmanhall and Leopardstown, Dublin, D18 P521, Irland	Betrieb von Servern und Cloud Server Netzwerken, Content Delivery Network zur Speicherung und Auslieferung von Audio / Video Streams,
1&1 IONOS SE Elgendorfer Str. 57, 56410 Montabaur	Betrieb von Servern und Cloud Server Netzwerken, Content Delivery Network zur Speicherung und Auslieferung von Webseiten und Webinhalten und Datenbanken,
TenshiTec Neustift 7, 85622 Weißenfeld	Serveradministration und Entwicklung

Anlage: Erfasste, gespeicherte und verarbeitete Daten

IMS erfasst, speichert und verarbeitet Daten wie folgt:

Daten	Szenario	Rechts-grundlage	Zugriff	Speicherung und Löschung
Audio/Video Streams	Serverseitig können eingehende Live A/V Signale aufgezeichnet werden	Auftrags-erfüllung	Eigentümer/Kunde	Speicherung innerhalb der Plattform bis zur Löschung des Webcast Projektes (manuell oder automatisch nach Ablauf der entsprechenden Fristen)
Teilnehmer Daten	Im Zuge der Anmeldung können beliebige Teilnehmerdaten abgefragt und gespeichert werden	Auftrags-erfüllung	Eigentümer/Kunde, Teilnehmer (optional können Teilnehmerdaten innerhalb des Webcasts angezeigt werden – Details siehe Pkt. Teil-nehmerverwaltung	
Eingehende Nachrichten, Informationen	Der Kunde kann eigene sowie vom System bereit gestellte Funktionalitäten zur Dateneingabe durch den Teilnehmer nutzen.	Auftrags-erfüllung		

Technisch-organisatorische Maßnahmen

gemäß DSGVO

Inhaltsverzeichnis

Datenverarbeiter

InterMedia Solutions GmbH
(nachstehend IMS genannt)
Ahornstr. 7, 82041 Oberhaching bei München

Ansprechpartner: Robert Holzer
Tel: +49 89-244 151 51
E-Mail: datenschutz@intermedia-solutions.de

1.0 Vertraulichkeit

1.1 Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Technische Maßnahmen: Klingelanlage mit Kamera, Sicherheitsschlösser, Manuelles Schließsystem, Alarmanlage, Videoüberwachung der Eingänge.

Organisatorische Maßnahmen: Besucher in Begleitung durch Mitarbeiter, Sorgfalt bei Auswahl Reinigungsdienste, Schlüsselregelung

1.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Technische Maßnahmen: Login mit Benutzername + Passwort, Anti-Viren-Software Server, Anti-Viren-Software Clients, Firewall, Einsatz VPN bei Remote-Zugriffen, Verschlüsselung von Datenträgern, Automatische Desktopsperre, Verschlüsselung von Notebooks,

Organisatorische Maßnahmen: Erstellen von Benutzerprofilen, Zentrale Passwortvergabe, Richtlinie „Sicheres Passwort", Allg. Richtlinie Datenschutz

1.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Technische Maßnahmen: Protokollierung von Zugriffen

Organisatorische Maßnahmen: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte

1.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Technische Maßnahmen: Trennung von Produktiv- und Testumgebung, Physikalische Trennung (Systeme / Datenbanken / Datenträger)

Organisatorische Maßnahmen: Steuerung über Berechtigungskonzept, Festlegung von Datenbankrechten

2.0 Integrität

2.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Technische Maßnahmen: Technische Protokollierung der Eingabe, Änderung und Löschung von Daten, Manuelle oder automatisierte Kontrolle der Protokolle

Organisatorische Maßnahmen: Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts, Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden

2.2 Eingangskontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.
Technische Maßnahmen: Email-Verschlüsselung, Einsatz von VPN, Protokollierung der Zugriffe und Abrufe, Bereitstellung über verschlüsselte Verbindungen wie sftp und https, elektronische Signaturen

Organisatorische Maßnahmen: Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen, Weitergabe in anonymisierter oder pseudonymisierter Form, Sorgfalt bei Auswahl von Transport Personal und Fahrzeugen

3.0 Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Technische Maßnahmen: Feuer- und Rauchmeldeanlagen, Feuerlöscher, Serverraumüberwachung, Serverraum klimatisiert, RAID System / Festplattenspiegelung, unterbrechungsfreie Stromversorgung

Organisatorische Maßnahmen: Backup-Strategie (online/offline; on-site/off-site), Kontrolle des Sicherungsvorgangs, Getrennte Partitionen für Betriebssysteme und Daten

4.0 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.1 Datenschutz-Maßnahmen

Technische Maßnahmen: Datenschutz-Management, Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt

Organisatorische Maßnahmen: Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet, Regelmäßige Sensibilisierung der Mitarbeiter, die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach

4.2 Incident-Response-Management

Technische Maßnahmen: Einsatz von Firewall und regelmäßige Aktualisierung, Einsatz von Spamfilter und regelmäßige Aktualisierung, Einsatz von Virenscanner und regelmäßige Aktualisierung

Organisatorische Maßnahmen: Vorgehensweise zum Umgang mit Sicherheitsvorfällen, Dokumentation von Sicherheitsvorfällen und Datenpannen

4.3 Datenschutzfreundliche Voreinstellungen

Technische Maßnahmen: Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind, Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen

4.4 Auftragskontrolle (Outsourcing an Dritte)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Organisatorische Maßnahmen: Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.