# Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

## 1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Zwischen Auftraggeber (Benutzer) und Auftragnehmer (Anbieter) besteht ein Vertragsverhältnis für die Nutzung der Plattform **GMC-Instruments.cloud** (Nutzungsvertrag), auf deren Grundlagen der Auftragnehmer Leistungen für den Auftraggeber erbringt. Konkret ermöglicht der Auftragnehmer dem Auftraggeber die Nutzung von **GMC-Instruments.cloud**. Im Rahmen der Nutzung von **GMC-Instruments.cloud** erhält der Auftragnehmer Kenntnis von personenbezogenen Daten, die von dem Auftraggeber stammen und ausschließlich für diesen verarbeitet werden. Die Einzelheiten, auch im Hinblick auf den Umfang der Nutzung von **GMC-Instruments.cloud** und den Bestand an personenbezogenen Daten, ergeben sich aus den Nutzungsbedingungen.

Die Vereinbarung zur Auftragsverarbeitung und die Nutzungbedingungen sind voneinander abhängig; insbesondere kann die AVV nicht separat gekündigt werden.

Die AVV hat Vorrang vor allen abweichenden Bestimmungen, die in anderen Vereinbarungen zwischen den Parteien, einschließlich einer Leistungsvereinbarung, enthalten sind.

(2) Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Nutzungsvereinbarung.

## 2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Der Auftraggeber erfasst Daten zum Zweck seiner weiteren Verarbeitung, die vom Auftragnehmer gespeichert werden.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet grundsätzlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Die unter 6. Unterauftragsverhältnisse bereits aufgeführten Anbieter aus Drittländern sind vom Auftragnehmer auf ein entsprechendes Datenschutzniveau geprüft worden.

Jede weitere Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DS-GVO erfüllt sind.

(2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

- ✓ Personenstammdaten
- ✓ Kommunikationsdaten (z.B. Telefon, E-Mail)



MCS Metra Cloud Services GmbH • Mercedesstraße 31 • D-71384 Weinstadt
Fon + 49 (0) 71 51 - 3 69 00-530 • info@gmc-instruments.cloud • www.audius.de

- ✓ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ✓ Kundenhistorie

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ✓ Kunden
- ✓ Abonnenten
- ✓ Beschäftigte
- ✓ Ansprechpartner

## 3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.
(2) Der Auftragnehmer hat die Sicherheit gem. Artt. 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 [Einzelheiten in Anlage 1].
(3) 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. Berichtigung, Einschränkung und Löschung von Daten

(1) 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.
(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.



MCS Metra Cloud Services GmbH • Mercedesstraße 31 • D-71384 Weinstadt
Fon + 49 (0) 71 51 - 3 69 00-530 • info@gmc-instruments.cloud • www.audius.de

## 5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

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

a) Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Der Auftragnehmer stellt dennoch eine verantwortliche Stelle zur Verfügung unter datenschutz@metracloudservices.de
b) Die Wahrung der Vertraulichkeit gemäß Artt. 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 Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].
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 in Anspruch nimmt, z.B. Telekommunikationsleistungen, Post-/Transportdienstleistungen, Reinigungsleistungen oder Bewachungsdienstleistungen. Wartungs- und



MCS Metra Cloud Services GmbH • Mercedesstraße 31 • D-71384 Weinstadt
Fon + 49 (0) 71 51 - 3 69 00-530 • info@gmc-instruments.cloud • www.audius.de

Prüfleistungen stellen dann ein Unterauftragsverhältnis dar, wenn sie für IT-Systeme erbracht werden, die im Zusammenhang mit einer Leistung des Auftragnehmers nach diesem Vertrag erbracht werden und der Auftragnehmer im Rahmen dieser zumindest die Möglichkeit der Kenntnisnahme personenbezogener Daten erhält. 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 zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer setzt unterschiedliche Unterauftragnehmer (weitere Auftragsverarbeiter) ein.

| Firma Unterauftragnehmer | Anschrift/Land | Leistung |
|---|---|---|
| audius GmbH | audius GmbH<br>Mercedesstraße 31<br>71384 Weinstadt<br>Germany | Kooperationspartner und Anbieter von ELEXONIQ.<br>Vertragsmanagement |
| audius SE | audius SE<br>Mercedesstraße 31<br>71384 Weinstadt<br>Germany | Unternehmen der audius Gruppe.<br>Durchführung von Abrechnungen |
| Gossen Metrawatt GmbH | Gossen Metrawatt GmbH<br>Südwestpark 15<br>90449 Nürnberg<br>Germany | Kooperationspartner Cloud und Anbieter von IZYTRONIQ. |
| GMC-I Service GmbH | GMC-I Service GmbH<br>Beuthener Straße 41<br>90471 Nürnberg<br>Germany | Anbieter der Cloud Bausteine und Produkte der GMC-I Service GmbH |
| Microsoft | Microsoft Ireland Operations Limited<br>South County Business Park<br>Leopardstown<br>Dublin 18,<br>Ireland | Hosting und Bereitstellung von Server und IT-Infrastruktur. |
| Auth0 | Okta, Inc.,<br>Attn: Legal Team,<br>100 First Street,<br>Floor 6,<br>San Francisco, CA 94105<br>USA | Verwaltung der Benutzer-Anmeldedaten der Plattform. |

Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.



MCS Metra Cloud Services GmbH • Mercedesstraße 31 • D-71384 Weinstadt
Fon + 49 (0) 71 51 - 3 69 00-530 • info@gmc-instruments.cloud • www.audius.de

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.
(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.
(5) Der Auftragnehmer nimmt keinen Unterauftragnehmer ohne vorherige schriftliche konkrete oder allgemeine Genehmigung des Auftraggebers in Anspruch. Der Auftragnehmer informiert den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Unterauftragnehmern. Der Auftraggeber hat die Möglichkeit innerhalb einer angemessenen Frist Einspruch zu erheben. Verweigert der Auftraggeber durch seinen Einspruch die Zustimmung aus anderen als aus wichtigen Gründen und finden die Vertragsparteien keine einvernehmliche Regelung, kann der Vertrag außerordentlich gekündigt werden.

## 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 während der üblichen Geschäftszeiten 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 der technisch-organisatorischen Maßnahmen zur Einhaltung der besonderen Anforderungen des Datenschutzes allgemein sowie solche, die den Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

## 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



MCS Metra Cloud Services GmbH • Mercedesstraße 31 • D-71384 Weinstadt
Fon + 49 (0) 71 51 - 3 69 00-530 • info@gmc-instruments.cloud • www.audius.de

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.



MCS Metra Cloud Services GmbH • Mercedesstraße 31 • D-71384 Weinstadt
Fon + 49 (0) 71 51 - 3 69 00-530 • info@gmc-instruments.cloud • www.audius.de

# Anlage – Technisch-organisatorische Maßnahmen

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

- Zutrittskontrolle
  Geschäftsräume der audius Gruppe sind durch elektronische Zutrittskontrollsysteme, Schlüsselsysteme und/oder einen besetzten Empfang geschützt.
  Die Ausgabe von Magnet- oder Chipkarten und Schlüsseln wird dokumentiert, die freigeschalteten Bereiche entsprechen der Funktion des Empfängers.
  Besonders sensible Bereiche sind zusätzlich über Alarmanlagen sowie Videoüberwachung geschützt.

  Beispiele aus dem Katalog der umgesetzten Maßnahmen:
  - Magnet- oder Chipkarten
  - Schlüssel
  - elektrische Türöffner
  - Alarmanlagen
  - Videoanlagen

- Zugangskontrolle
  audius verhindert, dass Datenverarbeitungssystem von Unbefugten genutzt werden können, indem Zugangswege abgesichert und beschränkt sowie persönliche Zugangsberechtigungen vergeben werden. Die Zugangskontrolle zu den Kundensystemen erfolgt über eine logische Abtrennung des Kundennetzwerks bzw. Rechenzentrumsnetzwerks zum Internen Netzwerk. Über eine User-Passwort-Authentifizierung wird der Zugang entsprechend des Berechtigungskonzeptes personenbezogener User gewährt und protokolliert. Ist ein Kundensystem über öffentliche Netze erreichbar, so ist ein Sicherheitskonzept für den externen Zugang eingerichtet. Der audius Standarduser hat keine Administrationsrechte.
  Sicherheitsrelevante Benutzerkonten werden regelmäßig überprüft. Es gibt eindeutige Benutzerkonten und keine Sammelkonten. Eine Passwort Policy (Passwortrichtlinie) ist vorhanden.

  Beispiele aus dem Katalog der umgesetzten Maßnahmen:
  - Das Prinzip der minimalen Berechtigung ist vorhanden.
  - Die Eingabe des Passwortes muss unbeobachtet erfolgen.
  - Die Default Passwörter müssen geändert werden.
  - Es gibt keine Gruppen oder gemeinsam genutzte Passwörter.
  - Festgelegte Passwortkomplexität mit Passwort-Historie.
  - Die Sperrung des Accounts erfolgt nach x ungültigen Versuchen.
  - Eine Entsperrung kann nur durch den Administrator nach vorheriger Prüfung erfolgen.
  - Alle Zugriffe und Zugriffsversuche werden im Systemlog gespeichert.
  - Bei nicht benutzten Sitzungen erfolgt nach x Minuten ein timeout.
  - Passwörter dürfen weder schriftlich noch elektronisch im Klartext oder unverschlüsselt hinterlegt werden. Ausnahme bilden Notfallpasswörter, die im Safe hinterlegt werden, wenn dies vertraglich vereinbart ist. Es gibt ein Verbot der Mehrfachänderungen sowie ein Mitteilungsverbot.
  - Automatische Sperrung des Arbeitsplatzrechners
  - Einrichtung eines Benutzerstammsatzes pro User
  - Verschlüsselung von Datenträgern



MCS Metra Cloud Services GmbH • Mercedesstraße 31 • D-71384 Weinstadt
Fon + 49 (0) 71 51 - 3 69 00-530 • info@gmc-instruments.cloud • www.audius.de

- Zugriffskontrolle
  audius gewährleistet, dass die zur Nutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsbefugnis unterliegenden Daten zugreifen können. Durch Rollenvergabe und das Arbeiten mit Benutzerprofilen ist dies sichergestellt. Die Benutzerprofile werden in regelmäßigen Abständen vom Verantwortlichen überprüft und ggf. angepasst. Anpassungen an veränderte Personal- und Projektsituationen erfolgen nach einem vorgegebenen Prozess. Ferner wird sichergestellt, dass personenbezogene Daten bei der Verarbeitung und Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Auf den Arbeitsplatzrechnern werden keine Sicherheitsrelevanten Kundendatensätze gespeichert. Kundendatensätze werden ausschließlich auf vordefinierten Laufwerken verarbeitet. Alle Arbeitsplatzrechner sind mit einem Passwortschutz versehen.

  Beispiele aus dem Katalog der umgesetzten Maßnahmen:
  - Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte
  - Protokollierung von Zugriffen;

- Trennungskontrolle
  Bei audius erfolgt eine getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden z. B. durch:
  - Mandantenfähigkeit
  - Virtualisierung
  - Getrennte Dienstleister

- Pseudonymisierung
  Wo möglich, wird bei audius mit Pseudonymisierung gearbeitet. D. h. die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

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

- •Weitergabekontrolle
  audius verzichtet auf den physischen Transport von Datenträger. Dieser erfolgt ausschließlich auf Wunsch des Kunden unter den dann zu bestimmenden Sicherheitsvorkehrungen. Ein Prozedere wird hierzu mit dem Kunden gemeinsam definiert und dokumentiert.
  audius stellt sicher, dass personenbezogene Daten bei der elektronischen Übertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Bei Erfordernis werden die Daten dazu verschlüsselt.
  Für die Entsorgung von Datenträgern ist eine Sicherheitsstufe festgelegt.
  Datenträger (Papier, CD etc.) werden nur von zertifizierten Entsorgungsbetrieben vernichtet. audius erhält vom Entsorgungsbetrieb die entsprechenden Protokolle und Zertifikate.

  Beispiele aus dem Katalog der umgesetzten Maßnahmen:
  - Verschlüsselung
  - Virtual Private Networks (VPN)

- Eingabekontrolle



MCS Metra Cloud Services GmbH • Mercedesstraße 31 • D-71384 Weinstadt
Fon + 49 (0) 71 51 - 3 69 00-530 • info@gmc-instruments.cloud • www.audius.de

Auftraggeber-Daten können nicht von unbefugten Dritten oder Mitarbeitern von audius ergänzt bzw. verändert werden. Dies ist sichergestellt durch eine entsprechende Verpflichtung der Mitarbeiter des Auftragnehmers und die Einrichtung und Umsetzung von Zutritts-/, Zugangs- und Zugriffskontrollen. Darüber hinaus werden Benutzeraktionen im System bei Datenneueingaben, Datenänderungen und Datenlöschungen protokolliert, sofern das System dies vorsieht.

Beispiele aus dem Katalog der umgesetzten Maßnahmen:

- Protokollierung
- Dokumentenmanagement

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

- Verfügbarkeitskontrolle
  Personenbezogene Daten sind gegen zufällige oder mutwillige Zerstörung bzw. Verlust geschützt.
  Im vorhandenen Datensicherungskonzept ist die Verfahrensweise für die Datensicherung geregelt. In diesem Dokument ist definiert, in welchen Intervallen Datensicherungen durchgeführt werden, wie lange die Vorhaltung und die Aufbewahrungszeiten sind und wie die Auslagerung – in unterschiedlichen Gebäuden und Brandabschnitten – erfolgt.
  Die Sekundärenergieversorgung des Rechenzentrums wird durch USVs aufrechterhalten.

  Beispiele aus dem Katalog der umgesetzten Maßnahmen:
  - 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
  Die für und im Rahmen des Auftrags verarbeiteten personenbezogenen Auftraggeber-Daten werden nur entsprechend den vertraglichen Vereinbarungen mit dem Auftraggeber oder dessen Einzelanweisungen verarbeitet. Die Aufbau- und Ablauforganisation innerhalb des Auftragnehmers ist diesen Erfordernissen angepasst und mit wirksamen Kontrollmechanismen versehen. audius hat einen betrieblichen Datenschutzbeauftragten bestellt und sorgt durch die Datenschutzorganisation für dessen angemessene und effektive Einbindung in die relevanten betrieblichen Prozesse, welche regelmäßig bzw. bei sicherheitsrelevanten Vorkommnissen sofort durch interne Audits geprüft werden.
  Schulungen der Mitarbeiter zur Einhaltung der relevanten Datenschutz-Gesetze sowie hinsichtlich der Informationssicherheit werden regelmäßig durchgeführt. Eine Verpflichtung der Mitarbeiter auf die Vertraulichkeit findet bei Aufnahme der Tätigkeit statt.



MCS Metra Cloud Services GmbH • Mercedesstraße 31 • D-71384 Weinstadt
Fon + 49 (0) 71 51 - 3 69 00-530 • info@gmc-instruments.cloud • www.audius.de

Beispiele aus dem Katalog der umgesetzten Maßnahmen:

- Eindeutige Vertragsgestaltung
- formalisiertes Auftragsmanagement
- strenge Auswahl des Dienstleisters



MCS Metra Cloud Services GmbH • Mercedesstraße 31 • D-71384 Weinstadt
Fon + 49 (0) 71 51 - 3 69 00-530 • info@gmc-instruments.cloud • www.audius.de