

## ADV-VERTRAG | AUFTRAGSVERARBEITUNG

Dieser Vertrag regelt die datenschutzrechtlichen Pflichten des Auftragnehmers:

ViaConsilium GmbH  
Zu den Fußfällen 80  
50259 Pulheim  
(+49) 2238 - 4568292  
(nachfolgend: Auftragnehmer)

und der

xxx

xxx

00000 xxx

(nachfolgend: Auftraggeber)

1. Der Gegenstand und die Dauer des Auftrags, die Art und der Zweck der Verarbeitung, die Art der Daten und die Kategorien der Betroffenen ergeben sich aus dem Hauptvertrag (bestehend aus AGB der MM, gebuchter (= zuordbarer) Paketeleistungsbeschreibung [i.d.R. Basis, Plus, Enterprise], Informationen aus der VC-Auftragsbestätigung und der Anlage 2 des ADV-Vertrags zwischen den Parteien. Der Auftrag endet mit Beendigung des Hauptvertrages und der Erfüllung der Pflichten nach Ziffer 9.

2. Der Auftragnehmer hält in seinem Verantwortungsbereich die vereinbarten technischen und organisatorischen Maßnahmen gemäß Art.5 Abs. 1 und Art. 32 DSGVO ein und hat seine innerbetriebliche Organisation gemäß datenschutzrechtlichen Anforderungen gestaltet.

3. Der Auftragnehmer hat nur nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen oder zu löschen oder die Verarbeitung einzuschränken. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten oder der Einschränkung der Verarbeitung wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

Im Rahmen des Geschäftsgegenstandes des Produktes „Assentior“ ist es in der Regel der Betroffene selbst, der seine Daten einpflegt, freigibt bzw. ändert (im Kern: Einwilligungen erteilen oder entziehen, generelle Einverständnisverweigerung, Adressänderung).

Der Auftragnehmer wird den Auftraggeber im Falle der Geltendmachung gesetzlicher Betroffenenrechte unterstützen; dies umfasst insbesondere die Unterstützung bei der Beantwortung von Anträgen auf Wahrung der Betroffenenrechte mittels geeigneter technisch-organisatorischer Maßnahmen.

4. Der Auftragnehmer gewährleistet die Einhaltung der folgenden Pflichten:

- a) Schriftliche Bestellung – soweit gesetzlich vorgeschrieben – eines Datenschutzbeauftragten. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Sofern ein Wechsel in der Person des Datenschutzbeauftragten stattfindet, wird dies dem Auftraggeber unverzüglich mitgeteilt.
- b) Alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, müssen schriftlich zur Vertraulichkeit verpflichtet sein und über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehrt werden. Auf Anfrage des Auftraggebers wird der Auftragnehmer diesem die Verpflichtungserklärungen vorlegen. Dies ist nicht notwendig, soweit für die betreffenden Personen eine angemessene gesetzliche Verschwiegenheitspflicht besteht.
- c) Duldung öffentlicher Kontrollen durch die zuständigen Datenschutzaufsichtsbehörden in gleichem Umfang, wie die Datenschutzaufsichtsbehörden Prüfungen beim Auftraggeber durchführen dürfen. Unterstützung des Auftraggebers bei Kontrollen und Anfragen der Aufsichtsbehörden.
- d) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde. Dies gilt auch, soweit eine zuständige Behörde nach Art. 82 ff. DSGVO bei dem Auftragnehmer ermittelt.
- e) Die angemessene Unterstützung des Auftraggebers bei der Gewährleistung der Sicherheit der Verarbeitung gem. Art. 32 DSGVO.
- f) Die angemessene Unterstützung des Auftraggebers bei Datenschutz-Folgenabschätzungen gem. Art. 35 DSGVO und bei der vorherigen Konsultation der zuständigen Datenschutzaufsichtsbehörden nach Art. 36 DSGVO.
- g) Die angemessene Unterstützung des Auftraggebers bei der Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde (Art. 33 DSGVO) und bei der Benachrichtigung der von Verletzungen des Schutzes personenbezogener Daten betroffenen Personen (Art. 34 DSGVO).
- h) Die Vorlage der nach Art. 30 Abs. 2 DSGVO (Verzeichnis von Verarbeitungstätigkeiten) erforderlichen Angaben.

5. Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglichen Leistungen verbundenen Unternehmen Unteraufträge erteilt. Bei Erteilung eines Unterauftrags werden die vertraglichen Vereinbarungen zwischen Auftragnehmer und dem Unterauftragnehmer so gestaltet, dass sie den Anforderungen zu Datenschutz und Datensicherheit zwischen den Vertragspartnern dieses Vertrages entsprechen. Der Auftraggeber kann bei nachgewiesenen berechtigten Interessen einer Unterbeauftragung widersprechen.

Der Auftragnehmer erteilt der Auftraggeber auf dessen schriftliche Aufforderung hin Auskunft über den wesentlichen Vertragsinhalt (Leistungen ausschließlich Preise) und die Umsetzung der datenschutzrelevanten Pflichten des Unterauftragnehmers.

6. Die Verarbeitung der Daten durch den Auftragnehmer ist räumlich auf die EU und den EWR beschränkt.

Die Übermittlung von Daten durch den Auftragnehmer an einen Empfänger mit Sitz außerhalb des EWR ist nur unter den Voraussetzungen der Art. 44 ff. DSGVO zulässig und bedarf der gesonderten vorherigen schriftlichen Zustimmung des Auftraggebers. Der Auftragnehmer wird insbesondere sicherstellen, dass der Auftraggeber die Standardvertragsklauseln (vgl. z.B. die Entscheidung der Europäischen Kommission vom 5. Februar 2010, veröffentlicht im Amtsblatt der Europäischen Union L39/5, C (2010) 593; Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG) mit dem Empfänger der Daten abschließen kann.

7. Der Auftraggeber kann sich nach rechtzeitiger schriftlicher Anmeldung zu Prüfzwecken in den Betriebsstätten zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der technischen und organisatorischen Erfordernisse der für die Auftragsdatenverarbeitung einschlägigen Gesetze über den Datenschutz überzeugen. Der Auftragnehmer ist verpflichtet, die Kontrollen des Auftraggebers nach diesem Vertrag zu dulden, Mitwirkungsleistungen zu erbringen, soweit für die Kontrolle des Auftraggebers nach diesem Vertrag erforderlich, und dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist Auskünfte zu geben, die zur Durchführung einer umfassenden Auftragskontrolle erforderlich sind. Der Auftragnehmer ermöglicht dem Auftraggeber insbesondere, sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.

8. Der Auftragnehmer erstattet in allen Fällen dem Auftraggeber unverzüglich nach Kenntniserlangung eine Meldung, wenn durch ihn, die bei ihm beschäftigten Personen oder die von ihm eingesetzten Unterauftragnehmer Verstöße gegen Vorschriften zum Schutz der Daten des Auftraggebers (insbesondere die DSGVO) oder gegen die in dieser Vereinbarung getroffenen Festlegungen vorgefallen sind bzw. ein entsprechender Verdacht besteht. Der Auftragnehmer wird entsprechende Vorfälle dokumentieren, unverzüglich aufklären und Abhilfe schaffen. Er wird den Auftraggeber über den Fortgang der Angelegenheit bis zur Behebung des Vorfalls informiert halten. Sollte die Verletzung zu einem Risiko für die Rechte und Freiheiten der Betroffenen gem. Art. 33 DSGVO führen, wird der Auftragnehmer den Auftraggeber bei der Aufklärung des Vorfalls und im Rahmen der entsprechenden Meldung an die Datenschutzaufsichtsbehörde bzw. die Betroffenen umfassend unterstützen.

9. Der Umgang mit den von der Auftragsverarbeitung betroffenen Daten erfolgt im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers. Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung (gebuchtes Paket) ein Weisungsrecht über Art und Umfang der Datenverarbeitung vor, dass er durch Einzelweisungen konkretisieren kann. Abweichungen von Standardpaketleistungen sind für den Auftraggeber kostenpflichtig. U.a. deswegen sind Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen. Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen.

Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate 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. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer wird die Weisungen soweit erforderlich dokumentieren.

10. Vorbehaltlich abweichender Vereinbarungen und gesetzlicher oder satzungsmäßiger Pflichten ist der Auftragnehmer nach Vertragsende verpflichtet, ihm überlassene Datenträger an den Auftraggeber unverzüglich zurück zu geben und ihm in Zusammenhang mit dem Auftrag übergebene und noch nicht gelöschte personenbezogene Daten zu löschen. Über die Herausgabe oder Löschung nach Vertragsende muss der Auftraggeber innerhalb einer vom Auftragnehmer gesetzten Frist entscheiden. Wenn der Auftragnehmer zu vernichtende Unterlagen oder Datenträger mit personenbezogenen Daten dem Auftraggeber nicht zurückgibt, so ist der Auftragnehmer verpflichtet, die Unterlagen ordnungsgemäß zu entsorgen, ohne dass unbefugte Dritte von den Daten Kenntnis erlangen können. Entstehen beim Auftragnehmer nach Vertragsbeendigung Kosten durch die Herausgabe oder Löschung der Daten des Auftraggebers, so trägt diese der Auftraggeber.

Köln, den

Swisttal, den

\_\_\_\_\_  
Auftraggeber

\_\_\_\_\_  
Auftragnehmer

**Anlage 1: Technische und organisatorische Maßnahmen des Auftragnehmers (Art. 32 DSGVO, § 64 BDSG)**

- 1) Der Auftragnehmer hat unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.
- 2) Diese Maßnahmen können unter anderem die Pseudonymisierung und die Verschlüsselung personenbezogener Daten umfassen, soweit solche Mittel in Anbetracht der Verarbeitungszwecke möglich sind.
- 3) Die Maßnahmen sollen dazu führen, dass
  - a) die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt werden und,
  - b) dass die Verfügbarkeit personenbezogener Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.
- 4) Der Auftragsverarbeiter hat nach einer Risikobewertung Maßnahmen zu ergreifen, die Folgendes bezwecken:

**Zugangskontrolle**

Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte. Zweckmäßige Maßnahmen sind unter anderem:

- ✓ Zutrittskontrollsystem, zentrale Schlüsselverwaltung, Magnetkarte
- ✓ Schlüssel/Schlüsselvergabe ist zentral und organisatorisch klar geregelt
- ✓ Klare Zuweisung der Berechtigungen (Zugang Gebäude, Büro, Serverraum)
- ✓ Gebäudeschutz
- ✓ Regelungen für Besucher (Besucherausweis, Begleitung im Gebäude)
- ✓ Clean Desk Policy

**Datenträgerkontrolle**

Verhinderung des unbefugten Lesens, Kopierens, Veränderens oder Löschens von Datenträgern.

Zweckmäßige Maßnahmen sind unter anderem:

- ✓ Deziertes Kennwortverfahren zum Login [z.B. Klare Passwortregelung (bestimmte Länge, Kombination aus Buchstaben und Zahlen, keine Trivialpasswörter, Änderung in regelmäßigen Abständen). Voreingestellte Passwörter müssen umgehend geändert werden]
- ✓ Automatische Sperrung (z.B. Regelung zur automatischen Sperrung des Computers nach einer bestimmten Zeit der Inaktivität (mit anschließendem erneutem Login))
- ✓ Automatischer Standby-Betrieb der lokalen Rechner

- ✓ Verschlüsselung von Datenträgern möglich
- ✓ Besondere Vorsicht bei Mitnahme von Laptop/Datenträgern/Smartphones aus den Büroräumen heraus
- ✓ Möglichkeit der Fernlöschung von Smartphones

### **Speicherkontrolle**

Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten.

### **Benutzerkontrolle**

Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte.

### **Zugriffskontrolle**

Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben. Zweckmäßige Maßnahmen sind unter anderem:

- ✓ Differenzierte Berechtigungen (Profile, Rollen)
- ✓ Differenziertes Ordnerkonzept (z.B. alle Dateien sind einheitlich und nachvollziehbar zu benennen und so abzuspeichern, dass sie problemlos wiedergefunden werden können).
- ✓ Datenträger sind eindeutig zu kennzeichnen und sicher aufzubewahren.
- ✓ Sichere Löschung von Daten und/ oder Vernichtung von Datenträgern.
- ✓ Ordnung am Arbeitsplatz [Datenträger (USB-Sticks, CD-ROMs) mit vertraulichem Material dürfen nicht offen herumliegen].
- ✓ Anpassung sicherheitsrelevanter Standardeinstellungen von neuen Programmen und IT-Systemen
- ✓ Deinstallation bzw. Deaktivierung nicht benötigter sicherheitsrelevanter Programme und Funktionen (v.a. bei Smartphones)

### **Übertragungskontrolle**

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.

### **Eingabekontrolle**

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. Zweckmäßige Maßnahmen sind unter anderem:

- ✓ Protokollierungs- und Protokollauswertungssysteme werden eingesetzt
- ✓ Zugriff auf Datenverarbeitungssysteme nur nach Login möglich
- ✓ Keine Weitergabe von Passwörtern
- ✓ Zusätzlich zur automatischen Sperrung: manuelle Abmeldung beim Verlassen des Büros

**Transportkontrolle**

Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden. Zweckmäßige Maßnahmen sind unter anderem:

- ✓ Verschlüsselung (insbes. Laptops)
- ✓ Keine Benutzung von nicht freigegebener Hard-/ Software
- ✓ Keine Weiterleitung von E-Mails an private E-Mail-Accounts von Mitarbeitern
- ✓ Vorsicht beim Umgang mit Backup-Bändern
- ✓ Vorgaben an Mitarbeiter bzgl. Ausdrucken von geheimen Unterlagen
- ✓ Regelung zum Einsatz von USB-Sticks und CD-ROMs

**Wiederherstellbarkeit**

Gewährleistung, dass eingesetzte Systeme im Störfall wiederhergestellt werden können.

**Zuverlässigkeit**

Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

**Datenintegrität**

Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.

**Auftragskontrolle**

Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Zweckmäßige Maßnahmen sind unter anderem:

- ✓ Eindeutige Vertragsgestaltung
- ✓ Formalisierte Auftragserteilung
- ✓ Kriterien zur Auswahl des Auftragnehmers wird stringent eingehalten
- ✓ Kontrolle der Vertragsausführung wird durch den DSB gewährleistet

**Verfügbarkeitskontrolle**

Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind.

Zweckmäßige Maßnahmen sind unter anderem:

- ✓ Regelmäßiges Backup-Verfahren ist sichergestellt
- ✓ Getrennte Aufbewahrung von Daten ist gewährleistet
- ✓ Virenschutz/Firewall nach aktuellem Stand der Technik ist gewährleistet
- ✓ Schutz gegen Feuer, Überhitzung, Wasserschäden, Überspannung und Stromausfall im Serverraum
- ✓ Besondere Vorsicht bei Mitnahme von Laptop/Datenträger aus den Büroräumen heraus

**Trennbarkeit**

Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können. Zweckmäßige Maßnahmen sind unter anderem:

- ✓ Physisch und/oder logisch getrennte Speicherung, Veränderung, Löschung und Übermittlung von Daten, die unterschiedlichen Zwecken dienen (Mandantenfähigkeit)
- ✓ Funktionstrennung, insbesondere zwischen Produktions- und Testdaten

**Regelmäßige Überprüfung, Bewertung und Evaluierung der technischen und organisatorischen Maßnahmen**

- ✓ Regelmäßige fachliche Fortbildung der IT-Verantwortlichen und des betrieblichen Datenschutzbeauftragten
- ✓ Schulung der Mitarbeiter im Umgang mit der IT und zur Schärfung des IT-Sicherheitsbewusstseins
- ✓ Sicherheitshinweise werden allen Mitarbeitern in geeigneter Form bekannt gegeben und sind dauerhaft abrufbar (z.B. durch Veröffentlichung im Intranet)
- ✓ Auswertung von Meldungen und Berichten zu ungewöhnlichen Vorkommnissen
- ✓ Untersuchung erkannter oder vermuteter Verstöße gegen sicherheitsrelevante Vorgaben
- ✓ Regelmäßige Prüfung der Effektivität der bestehenden technischen und organisatorischen Maßnahmen und Prüfung, ob neue technische und organisatorische Maßnahmen erforderlich sind (beides unter Hinzuziehung des Datenschutzbeauftragten)
- ✓ Regelmäßige und anlassbezogene Kontrolle der Funktionalität der IT, einschließlich unter dem Aspekt der Zutrittskontrolle
- ✓ Eskalations- und Meldewege bei sicherheitsrelevanten Vorkommnissen
- ✓ Verfügbarkeit der IT-Verantwortlichen und des betrieblichen Datenschutzbeauftragten als Ansprechpartner bei allen Fragen zur IT-Nutzung und -sicherheit.

**Anlage 2: Datenschutzrechtliche Spezifikationen**

Umfang, die Art und der Zweck der vorgesehenen Erhebung

Der Auftragnehmer hostet die Daten des Produkts „Assentior“ und übernimmt die technische Betreuung. Seinerseits hat der Auftragnehmer das Unternehmen

ALL-INKL.COM - Neue Medien Münnich  
Hauptstraße 68  
02742 Friedersdorf

mit dem Datenhosting beauftragt. Der Auftragnehmer hat mit ALL-INKL.COM einen entsprechenden Auftragsverarbeitungsvertrag abgeschlossen.

Das Portal „Assentior“ vertreibt der Auftraggeber an seine Kunden (B2B, Vereine, etc.: nicht an Endkunden/Privatpersonen). Die Kunden können über das Portal Vorlagen, Wizzards und Dashboards nutzen bzw. selbst erstellte E-Mails und selbst erstellten Formularinhalte/Hinweise/Dokumente an ihre Mandanten versenden. Zu diesem Zweck werden in dem Portal Daten der Kunden und Daten deren Mandanten gespeichert.

Der Auftragnehmer hat im Rahmen des Hostings und der technischen Betreuung des Produkts Zugang zu den erhobenen Daten.

-----  
Der Auftragnehmer nutzt zu Abrechnungszwecken das Unternehmen

FastBill GmbH  
Wildunger Str. 6  
60487 Frankfurt am Main

Der Auftragnehmer hat mit FastBill einen entsprechenden Auftragsverarbeitungsvertrag abgeschlossen.

Verwendete Datenkategorien:

- Quellcode / technische Daten zum Portal Assentior (AN-MA)
- Zeitstempel, Nutzung Assentior (AN-MA, AG-MA, ADV)
- Accounts und Passwörter zum Portal Assentior (AN-MA, AG-MA, AG-K, ADV)
- Formularinhalte und -änderungen, Status; Portal Assentior (AN-MA, AG-MA, AG-K, ADV)
- Anhänge (Word, .pdf) (AG-MA, AN-MA, AG-K, ADV)
- E-Mail-Adressen (AG-MA, AN-MA, AG-K, ADV)
- Namen und Adressen (AG-MA, AN-MA, AG-K, ADV)
- Telefonnummer (AG-MA, AN-MA, ADV)
- E-Mail-Texte (AG-MA, AN-MA, AG-K, ADV)
- Bankverbindung (AG-MA, AN-MA, ADV)
- Bestelldaten (AG-MA, AN-MA, ADV)
- Kündigungsdaten (AG-MA, AN-MA, ADV)
- Rechnungsdaten und Zahlungsverhalten (AG-MA, AN-MA, ADV)
- Infos zu vertraglich vereinbarte Zusatzmodulen (AG-MA, AN-MA, ADV)
- Infos aus vertraglich vereinbarte Zusatzmodulen (AG-MA, AN-MA, AG-K, ADV)
- Löschinformationen (AG-MA, AN-MA, AG-K, ADV)

Betroffene:

Autorisierte Mitarbeiter des Auftragnehmers	AN-MA
Kunden des Auftraggebers	AG-K
Autorisierte Mitarbeiter des Auftraggebers	AG-MA
Auftragsdatenverarbeiter	ADV