Auftragsdatenverarbeitervereinbarung (ADV) für Umsetzung DSGVO, abgeschlossen

zwischen

Auftraggeber

Anschrift, PLZ Ort

in der Folge als „Auftraggeber“ bezeichnet und

APA-IT Informationstechnologie GmbH

Laimgrubengasse 10, 1060 Wien

in der Folge als „Auftragnehmer“ bezeichnet.

Präambel:

Um den zwingenden Bestimmungen der EU Datenschutzgrundverordnung 2016/679 (DSGVO) zu entsprechen, vereinbaren die Vertragsparteien einvernehmlich, dass alle vertraglichen Vereinbarungen zu datenschutzrechtlichen Themen in bestehenden Verträgen mit Wirkung zum 25.05.2018 durch die vorliegende Vereinbarung ersetzt werden, sofern die vorliegende Vereinbarung nichts Gegenteiliges vorsieht. Die Gültigkeit der übrigen Bestimmungen bleiben hiervon unberührt. Bei allfälligen Widersprüchen gehen die Bestimmungen der vorliegenden Vereinbarung vor.

I UMFANG DER AUFTRAGSVERARBEITUNG

1. Die Dauer der Verarbeitung richtet sich nach dem zivilrechtlichen Grundgeschäft, das der Auftragnehmer für den Verantwortlichen durchführt. Der Zweck der Verarbeitung, die Kategorien der betroffenen Personen sowie die Arten der personenbezogenen Daten richten sich nach dem jeweiligen Produkt und können unter https://www.apa.at/Site/Kontakt/Auftragsverarbeitung.de.html eingesehen werden.

II DATENSCHUTZ

1. Die Vertragsparteien verpflichten sich, die Regelungen des jeweils geltenden österreichischen und europäischen Datenschutzrechts einzuhalten. Der Auftragnehmer wird sämtliche Daten lediglich zu Zwecken der Vertragserfüllung für den Auftraggeber verwenden.
2. Der Auftragnehmer verpflichtet sich, personenbezogene Daten nur auf dokumentierte Weisung des Auftraggebers – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – zu verarbeiten, sofern der Auftragnehmer nicht durch das Recht der Union oder der Mitgliedstaaten, dem sie unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.
3. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung. Wenden sich Betroffene direkt an den Auftragnehmer, wird dieser das Ersuchen unverzüglich an den Auftraggeber weiterleiten. Der Auftragnehmer wird den Auftraggeber gem Art 28 Abs 3 lit h DSGVO informieren, falls der Auftragnehmer der Auffassung ist, dass eine Weisung gegen die DSGVO oder gegen andere geltende Datenschutzbestimmungen verstößt.
4. Die Vertragsparteien halten einvernehmlich fest, dass der Auftragnehmer über hinreichende Fachkenntnisse, Verlässlichkeit und Ressourcen verfügt und geeignete technische und organisatorische Maßnahmen so ergreift, dass die Anforderungen der DSGVO erfüllt werden.
5. Der Auftragnehmer leistet Gewähr, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben. Die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen bleibt auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.
6. Der Auftragnehmer erklärt rechtsverbindlich, dass er weitere Auftragsverarbeiter (Subverarbeiter) nur mit Billigung des Auftraggebers heranziehen wird, sofern die Erbringung der Hauptleistungen selbst, also die eigentliche Datenverarbeitung oder wesentlicher Teile davon, vertraglich verlagert bzw delegiert werden soll. Nicht als in diesem Sinne relevante Sub-Auftragsverhältnisse gelten daher zB allgemeine Hilfsdienstleistungen Dritter in den Bereichen Telekommunikation, Versand/Transport oder IT-Support, wobei allerdings immer für risikoangemessene und gesetzeskonforme Vertragsregelungen bzw Kontrollmaßnahmen zu sorgen ist. Dabei hat der Auftragnehmer dem Auftraggeber genaue Informationen über den Subverarbeiter zu geben und gegebenenfalls explizit darauf hinzuweisen, falls Daten ins Ausland überlassen werden. Nimmt der Auftragnehmer die Dienste eines Subverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten auszuführen, so werden diesem Subunternehmer im Wege eines Vertrags dieselben Datenschutzpflichten auferlegt, die in diesem Vertrag festgelegt sind.
7. Der Auftragnehmer verpflichtet sich, den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei zu unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Rechte der betroffenen Person entgeltlich nachzukommen. Insbesondere wird der Auftragnehmer erhaltene Anfragen, Beschwerden und Anträge von betroffenen Personen an den Verantwortlichen weiterleiten.
8. Der Auftragnehmer wird dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in dieser Vereinbarung niedergelegten Pflichten zur Verfügung stellen. Der Auftragnehmer wird – vorbehaltlich einer angemessen frühzeitig erfolgten schriftlichen Vorankündigung – dem Auftraggeber und/oder einem beauftragten Prüfer gestatten, Prüfungen und Inspektionen der Systeme und Prozesse des Auftragnehmers in Bezug auf die für den Auftraggeber verarbeiteten personenbezogenen Daten durchzuführen, sofern derartige Prüfungen und Inspektionen zu normalen Geschäftszeiten des Auftragnehmers und mit minimaler Störung ihres Geschäftsbetriebes erfolgen und alle dadurch gewonnenen Informationen durch den Auftraggeber streng vertraulich behandelt werden, sofern der Auftraggeber nicht zur Preisgabe dieser Informationen durch Gesetze verpflichtet ist. Alle Kosten, die dem Auftragnehmer im Zusammenhang mit der Zurverfügungstellung derartiger Informationen, Gestattung derartiger Prüfungen und Inspektionen und sonst im Zusammenhang mit diesem Vertragspunkt entstehen, werden vom Auftraggeber getragen.
9. Der Auftragnehmer verpflichtet sich nach Abschluss der Erbringung der Verarbeitungsleistungen, alle personenbezogenen Daten nach Wahl des Auftraggebers entweder zu löschen oder zurückzugeben, sofern nicht nach dem Unionsrecht oder dem Recht eines Mitgliedstaates der EU eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

III DATENSICHERHEIT

10. Bestehende Vereinbarungen betreffend die vom Auftragnehmer zu ergreifenden Datensicherheitsmaßnahmen bleiben durch diese Bestimmung unberührt und gelten unverändert weiter. Mögliche betragsmäßige Haftungsgrenzen richten sich nach dem dieser Vereinbarung zugrundeliegenden Grundvertrag.
11. Sofern zum Zeitpunkt dieser Vereinbarung keine bestehenden Abreden zu den zu ergreifenden Sicherheitsmaßnahmen getroffen wurden, gelten die in Anhang 1 beschriebenen Datensicherheitsmaßnahmen als ausreichend. Darüber hinaus können für konkrete Datenverarbeitungen weitergehende Maßnahmen vereinbart werden.
12. Der Auftragnehmer ist verpflichtet, die in Anhang 1 genannten Maßnahmen gegebenenfalls dem Stand der Technik anzupassen und den Auftraggeber hierüber zu informieren.
13. Der Auftragnehmer wird unter Berücksichtigung der Art der Verarbeitung und der ihr zur Verfügung stehenden Informationen den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten betreffend die Sicherheit personenbezogener Daten unterstützen.
14. Entgeltliche Leistungen: Alle vom Auftragnehmer zu erbringenden Tätigkeiten erfolgen generell gegen Entgelt. Sofern nicht im Grundvertrag anders geregelt, erfolgt die Verrechnung nach Aufwand nach den aktuellgültigen Stundensätzen der APA-IT.

Für den Auftraggeber:	**Für den Auftragnehmer:**
	Ing. Alexander Falchetto, MBA Geschäftsführer APA-IT
Name, Unterschrift	Name, Unterschrift
Wien, 23.3.2018	Wien, 23.3.2018
Ort, Datum	Ort, Datum

ANHANG ./1

APA-IT ist der kompetente Partner bei der Umsetzung und beim Betrieb von IT-Produkten. Datenschutz und Informationssicherheit stehen von jeher neben der Umsetzung und dem Betrieb von IT-Produkten im Zentrum unseres Handelns. APA-IT hat die Prozesse, die zum Betrieb der IT-Produkten dienen, umfassend zertifiziert.

Im Bereich der Informationssicherheit hat sich die Norm ISO/IEC 27001:2013 etabliert. Die Norm ISO/IEC 27001:2013 stellt Anforderungen an ein Informationssicherheitsmanagementsystem (ISMS), das dazu dient, Informationssicherheit in Prozessen zu berücksichtigen, die auch der Umsetzung von Kundenanforderungen dienen. Die APA-IT-Leitungsorgane haben sich selbst und ihre Mitarbeiter zur Einhaltung der Norm ISO/IEC 27001:2013 durch die Veröffentlichung von unternehmensinternen Richtlinien verpflichtet. Die Norminhalte werden regelmäßig geschult und im Rahmen von Audits, die sowohl von betriebsfremden, akkreditierten Stellen als auch von APA-IT-Mitarbeitern durchgeführt werden, auf deren Wirksamkeit hin geprüft. Die Norm ISO/IEC 27001:2013 entspricht dem Stand der Technik im Bereich der Informationssicherheit.

Durch die Einführung des ISMS kommt APA-IT auch den Verpflichtungen, die die Datenschutzgrundverordnung an die Datensicherheit stellt, nach. Aus datenschutzrechtlicher Sicht sind nachstehende technische und organisatorische Maßnahmen von besonderer Bedeutung, weil diese als eine Konkretisierung des abstrakten Begriffs der technischen und organisatorischen Maßnahmen der Datenschutzgrundverordnung (DSGVO) verstanden werden können. Zu diesen Maßnahmen zählt etwa die Zutrittskontrolle, die Zugangskontrolle, die Zugriffskontrolle, die Weitergabe- und Transportkontrolle, die Eingabekontrolle, die Auftragskontrolle, die Verfügbarkeitskontrolle und die Datenträgerkontrolle.

Die Maßnahmen im Einzelnen

Der **Zutrittskontrolle** kommt APA-IT dadurch nach, dass die Serverräumlichkeiten in einer eigenen Zone untergebracht sind. Der Zutritt ist durch eine Zutrittskontrolle abgesichert. Eine Videoüberwachungsanlage ist in Verwendung. Ausschließlich berechtigte Personen erhalten Zutritt. Der **Zugriffskontrolle** kommt APA-IT durch ein Berechtigungssystem nach. Es werden ausschließlich „named-User" verwendet. Die Zugriffsberechtigungen werden jährlich auf deren Angemessenheit geprüft. Die Zugriffsberechtigungen ergeben sich aus den Auftragsverarbeiterverträgen. Der **Protokollierungspflicht** und der **Eingabekontrolle** kommt APA-IT durch das Führen eines „Secure-Logs" oder durch die Protokollierung im Event-Log nach. Diese Log-Files dienen zur Erkennung einer rechtswidrigen Datenverwendung und zur Abwehr von Angriffen. Die Protokolle werden vom Chief Information Security Officer (CISO) entsprechend dem Auditplan geprüft. Der **Weitergabe- und Transportkontrolle** kommt APA-IT einerseits durch die Klassifikation der Informationen und andererseits durch die Verschlüsselung der mobilen Endgeräte nach. Die Kommunikation erfolgt über verschlüsselte Kanäle. Der Auftragsgebundenheit kommt APA-IT dadurch nach, dass Benutzer ausschließlich auf Systeme Zugriff erhalten, die zur Vertragserfüllung zu verwenden sind. IT-Richtlinien regeln den Umgang mit diesen Systemen. Der Verfügbarkeitskontrolle kommt APA-IT durch die redundante Führung des Rechenzentrumsbetriebs nach. Die Systeme werden nach den Vorgaben eines Backup-Konzeptes gesichert. Die Sicherungen werden auf deren Korrektheit geprüft. Die APA-IT-Mitarbeiter sind umfassend auf das Datengeheimnis verpflichtet. Diese Pflicht ist auch nach der Beendigung des Dienstverhältnisses einzuhalten.

Bestätigung der Wirksamkeit

TÜV AUSTRIA Deutschland GmbH (TÜV) hat das APA-IT-ISMS zertifiziert. TÜV selbst ist eine unabhängige, staatlich akkreditierte Zertifizierungsgesellschaft. Die Zertifikate sind unter dem unter Punkt 1 angeführten Link abrufbar.