WIRTSCHAFTSKAMMER WIEN
Die Kaffeehäuser

Auftragsverarbeiter-vereinbarung

Fachgruppe Wien der Kaffeehäuser
Sparte Tourismus und Freizeitwirtschaft

Auftragsverarbeitervereinbarung nach EUDSGVO

Vertragspartner

Verantwortlicher (früher Auftraggeber):

Vertreten durch:

Auftragsverarbeiter/Auftragnehmer (früher Dienstleister)

Vertreten durch:

Inhaltsverzeichnis

1 Einleitung

Diese Vereinbarung beschreibt die Rahmenbedingungen und einer sog. Auftragsverarbeitung i.S.d. EU Datenschutz Grundverordnung (EUDSGVO) sowie die Rechte und Pflichten der Vertragspartner (Verantwortlicher und Auftragsverarbeiter), im Folgenden auch Parteien genannt.

In diesem Dokument enthaltene Fachbegriffe und Definitionen sind der EUDSGVO entnommen und an sie angelehnt, bzw. sind in ihrem Sinne zu verstehen.

2 Gegenstand der Vereinbarung

2.1 Auftragsverarbeitung

[BESCHREIBUNG DER DURCHZUFÜHRENDEN AUFTRAGSVERARBEITUNG]

Anzugeben sind die beauftragte Verarbeitung, deren Dauer, der Zweck der Verarbeitung, die Art der Verarbeitung, die Arten der verarbeiteten personenbezogenen bzw. sensiblen Daten und die Betroffenen (Kategorien).

3 Rechte & Pflichten des Verantwortlichen (Auftraggeber)

Der Verantwortliche erteilt sämtliche Weisungen (Aufträge, Teilaufträge, etc.) in schriftlicher Form und dokumentiert diese zur Wahrung der Nachweisbarkeit. In sehr dringenden Fällen können Weisungen auch in mündlicher Form erteilt werden, müssen jedoch unverzüglich schriftlich dokumentiert und nochmalig bestätigt werden. Der Verantwortliche hat vor Beginn der Verarbeitung dem Auftragsverarbeiter eine Liste mit weisungsbefugten Personen, d.h. mit Personen, die dem Auftragsverarbeiter Weisungen erteilen dürfen, bekannt zu geben (Anlage 3).

Der Verantwortliche trägt die Verantwortung für die Rechtmäßigkeit der beauftragten Verarbeitung, die Einhaltung der aktuell gültigen Datenschutzgesetze sowie für die Wahrung der Betroffenenrechte und ist daher berechtigt, die Einhaltung dieser Gesetze und die Inhalte dieser Vereinbarung beim Auftragsverarbeiter zu kontrollieren. Dies kann durch den Verantwortlichen selbst oder durch von ihm beauftragte Dritte geschehen und muss in angemessenem Rahmen bleiben, d.h. darf den Regelbetrieb des Auftragsverarbeiters nicht entscheidend stören oder unterbrechen. Kontrollen erfolgen nach zeitlich angemessener Ankündigung und nach Möglichkeit zu den normalen Geschäftszeiten des Auftragsverarbeiters. Davon ausgenommen sind lediglich dringende und triftige Gründe („Gefahr im Verzug“), die vom Verantwortlichen auch entsprechend zu dokumentieren sind. Dies gilt auch für eventuelle Subauftragnehmer.

Der Nachweis der Einhaltung kann einerseits in Form der Bereitstellung entsprechender Dokumentationen durch den Auftragsverarbeiter oder andererseits in Form einer Kontrolle vor Ort beim Auftragsverarbeiter erfolgen. In erstem Fall ist der Auftragsverarbeiter verpflichtet, sämtliche Dokumentationen und Nachweise zu führen und bereitzustellen, die für eine datenschutzgerechte Kontrolle notwendig sind bzw. vom Verantwortlichen eingefordert werden. In Zweitem Fall ist der Auftragsverarbeiter verpflichtet, den Kontrollorganen des Verantwortlichen, unabhängig davon, ob es sich um Mitarbeiter des Verantwortlichen oder um von diesem beauftragte Dritte handelt, Zutritt und Einblick im Rahmen der Auftragsverarbeitung zu gewähren. Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich über die Ergebnisse der Kontrolle sowie über ev. festgestellte Fehler oder Unregelmäßigkeiten.

Der Verantwortliche ist dazu berechtigt, sich im Zweifelsfall an den vom Auftragsverarbeiter bekanntgegeben Datenschutzverantwortlichen oder Datenschutzbeauftragten zu wenden.

4 Rechte & Pflichten des Auftragnehmers

Der Auftragsverarbeiter ausschließlich dazu berechtigt, personenbezogene Daten wie vertraglich vereinbart zu verarbeiten. Ausnahmen bilden lediglich gesetzliche Verpflichtungen des Auftragsverarbeiters. Der Auftragsverarbeiter hat den Verantwortlichen über alle allfälligen gesetzlichen Verpflichtungen, die den Auftragsverarbeiter zu einer anderen als der vereinbarten Verarbeitung verpflichten, zu informieren, ausgenommen, ihm ist diese Information gesetzlich verboten. Andere als die vereinbarten Verwendungen, vor allem für eigene Zwecke, sind dem Auftragsverarbeiter strengstens untersagt.

Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind und er diese auch einhält. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung und er verpflichtet sich, sämtliche technische und organisatorische Maßnahmen (TOM, Anlage 1) nach dem Stand der Technik einzusetzen und zu dokumentieren, die den Datenschutz gewährleisten. Der Auftragsverarbeiter verpflichtet sich dazu, die Verarbeitung der Daten ausschließlich innerhalb der EU durchzuführen. Verarbeitungen außerhalb der EU bedürfen der ausdrücklichen Zustimmung des Verantwortlichen. Sollte der Auftragsverarbeiter selbst nicht in der EU niedergelassen sein, so hat er einen verantwortlichen Ansprechpartner innerhalb der EU sowie Änderungen dieser Person vor Beginn der Verarbeitung bekanntzugeben. Dies gilt auch für Subauftragnehmer. Weiters verpflichtet sich der Auftragsverarbeiter dazu, das Datengeheimnis und die Vertraulichkeit bei sich selbst und allen seinen Mitarbeiter strengstens einzuhalten.

Der Auftragsverarbeiter bestätigt nachweislich, dass alle Personen, die im Zuge des Auftrages bzw. der Auftragsverarbeitung Kenntnis von den im Auftrag verarbeiteten Daten erhalten oder erhalten könnten, vor Beginn der Verarbeitung, mit den Bestimmungen der aktuellen Datenschutzgesetze und dieser Vereinbarung vertraut gemacht wurden und sie sich schriftlich zur Geheimhaltung verpflichtet haben, sofern sie nicht aus Berufsgründen oder gesetzlich einer besonderen Geheimhaltungspflicht unterliegen. Er weist weiters nach, dass diese Personen regelmäßigen Schulungen und Sensibilisierungen i.S.d. Datenschutzes unterliegen und er die Einhaltung des Datenschutzes im Rahmen der Auftragsverarbeitung überwacht. Dies gilt auch für eventuelle Subauftragnehmer. Der Auftragsverarbeiter hat sich, vor Beginn der Verarbeitung bei einem Subauftragnehmer sowie mindestens einmal jährlich, nachvollziehbar von der Einhaltung und Überwachung der aktuellen Datenschutzgesetze sowie der Vereinbarungen im Rahmen dieser Auftragsverarbeitung, nachweislich zu überzeugen. Die Ergebnisse sind dem Verantwortlichen unverzüglich mitzuteilen. Verstößt der Subauftragnehmer nachweislich gegen die ihm auferlegten Vorgaben, Regeln und Pflichten, so haftet der Auftragsverarbeiter dafür dem Verantwortlichen gegenüber.

Der Auftragsverarbeiter hat sämtliche von ihm im Rahmen dieser Auftragsverarbeitung eingesetzten Subauftragnehmer vor Beginn der Verarbeitung dem Verantwortlichen bekanntzugeben (Anlage 2). Die in dieser Liste angegebenen Subauftragnehmer gelten mit Unterfertigung dieser Vereinbarung als genehmigt. Die Beauftragung zusätzlicher Subauftragnehmer, sofern sie die Verarbeitung dieser Vereinbarung betreffen und nicht nur für systemerhaltende Dienstleistungen (Transport, Systemwartung,) beim Auftragsverarbeiter benötigt werden, ist nur mit schriftlicher Zustimmung des Verantwortlichen gestattet.

Der Auftragsverarbeiter verpflichtet sich, den Weisungen des Verantwortlichen im Rahmen dieser Auftragsverarbeitung jederzeit und unverzüglich Folge zu leisten. Dies gilt auch über die Beendigung dieser Vereinbarung hinaus. Der Auftragsverarbeiter wird Weisungen nur von den Personen annehmen und ausführen, die ihm vom Verantwortlichen bekannt gegeben wurden (Anlage 3). Weiters wird der Auftragsverarbeiter dem Verantwortlichen die Personen mitteilen, die berechtigt sind, Weisungen anzunehmen (Anlage 3). Eventuelle Verhinderungen, die eine Vertretung notwendig machen, z.B. bei Krankheit, Urlaub oder Wechsel der Person, sind

beiderseits zeitnah bekannt zu geben. Sollte der Auftragsverarbeiter der Meinung sein, dass Weisungen des Verantwortlichen gegen gültige Gesetze oder die Bestimmungen dieser Vereinbarung verstoßen, so hat er den Verantwortlichen unverzüglich schriftlich darauf hinzuweisen. Der Auftragsverarbeiter ist daraufhin berechtigt, die Ausführung der Weisung solange auszusetzen, bis der Verantwortliche die Sachlage geklärt und die Weisung entweder bestätigt oder geändert hat.

Der Auftragsverarbeiter gibt dem Verantwortlichen vor Beginn der Verarbeitung eine für den Datenschutz beim Auftragsverarbeiter verantwortliche Person, oder einen Datenschutzbeauftragten, sofern der Auftragsverarbeiter zur Bestellung eines solchen gesetzlich verpflichtet ist, bekannt. Änderungen in dieser Person sind dem Verantwortlichen unverzüglich mitzuteilen. Sollte der Auftragsverarbeiter keine solche Person bestellt oder definiert haben, so hat er den Grund dafür vor Beginn der Verarbeitung schriftlich zu begründen.

Die von der EUDSGVO geforderte Erstellung eines Verarbeitungsverzeichnisses sowie die Durchführung von Datenschutz Folgeabschätzungen durch den Verantwortlichen sind vom Auftragsverarbeiter nach Kräften zu unterstützen. Vom Verantwortlichen dafür benötigte Informationen und Dokumentationen sind vom Auftragsverarbeiter zu führen und auf Anforderungen unverzüglich bereitzustellen.

Sollte dem Auftragsverarbeiter gegenüber Betroffenenrechte geltend gemacht werden, so ist der Verantwortliche darüber unverzüglich zu informieren. Dies gilt auch, falls der Auftragsverarbeiter einer Kontrolle unterzogen wird, z.B. durch Aufsichtsbehörden. Der Auftragsverarbeiter ist nicht dazu berechtigt, Betroffenen gegenüber Auskunft zu erteilen, oder auf Anforderung dieser Daten zu löschen, außer er verfügt dafür über die ausdrückliche Zustimmung des Verantwortlichen. Eventuelle Anfragen oder Begehren durch Betroffene hat der Auftragsverarbeiter unverzüglich dem Verantwortlichen weiterzuleiten. Weiters ist der Auftragsverarbeiter nicht dazu berechtigt, Daten im Rahmen dieser Vereinbarung bzw. dieser Auftragsverarbeitung, ohne ausdrückliche Zustimmung des Verantwortlichen, zu verändern (berichtigen), zu löschen zu sperren oder auf andere Art unzugänglich zu machen.

Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich über Verletzungen der aktuell gültigen Datenschutzgesetze im Rahmen der Auftragsverarbeitung bei ihm oder anderswo, oder auch nur über den begründeten Verdacht hierzu, zu informieren. Die Information hat alle Angaben lt. Art. 33 Abs. 3 EUDSGVO zu enthalten. Generell sichert der Auftragsverarbeiter zu, den Verantwortlichen in allen Pflichten der Art. 33 und Art. 34 EUDSGVO zu unterstützen. Weiters ist der Verantwortliche über sämtliche Störungen in der Auftragsverarbeitung und deren Gründe unverzüglich zu informieren.

Eine gesonderte Vergütung für die Aufwände zur Erfüllung seiner Verpflichtungen steht dem Auftragsverarbeiter nicht zu. Diese ist in einem allfälligen Hauptvertrag zu regeln.

5 Technische und organisatorische Maßnahmen

Die in Anlage 1 beschriebenen technischen und organisatorischen Maßnahmen dienen der Aufrechterhaltung des Datenschutzes und werden im Zuge dieser Auftragsverarbeitung als zu betreibendes Mindeststandard betrachtet und sind vom Auftragsverarbeiter einzuhalten. Der Nachweis der Einhaltung ist regelmäßig, jedoch mindestens einmal jährlich, zu erbringen. Da diese Maßnahmen der technischen und organisatorischen Weiterentwicklung unterliegen, ist der Auftragsverarbeiter berechtigt, dies auch entsprechend dem Stand der Technik zu verändern, solange der vereinbarte und für die Auftragsverarbeitung benötigte Mindeststandard nicht unterschritten wird. Über eventuelle Änderungen ist der Verantwortliche vor deren Inbetriebnahme zu informieren. Sollte der Mindeststandard im Zuge der Inbetriebnahme unterschritten werden, so hat der Verantwortliche ein Vetorecht.

Sämtliche personenbezogenen Daten im Zuge der Auftragsverarbeitung sind strikt von anderen Daten, z.B. von anderen Kunden des Auftragsverarbeiters, physikalisch oder mit geeigneten virtuellen Mitteln, zu trennen. Die Erstellung von Kopien oder Duplikaten durch den Auftragsverarbeiter ist, sofern es sich nicht um technisch notwendige Vervielfältigungen oder Datensicherungen, zu denen der Auftragsverarbeiter gesetzlich verpflichtet ist, handelt, untersagt. Eventuell im Zuge dessen erstellte oder vom Verantwortlichen bereitgestellte Datenträger sind speziell zu kennzeichnen, datenschutzgerecht aufzubewahren und der Zugriff durch unbefugte Personen ist zu verhindern. Die Handhabung ist zu dokumentieren.

Die Verarbeitung personenbezogener Daten des Verantwortlichen durch Mitarbeiter des Auftragsverarbeiters oder dessen Subauftragnehmer in Privatbereichen (Privatwohnung), auf privaten Geräten oder in öffentlichen Bereichen, ist strengstens untersagt. Ausnahmen sind vom Verantwortlichen schriftlich zu genehmigen.

6 Beendigung der Auftragsverarbeitung

Nach jeglicher Beendigung der Auftragsverarbeitung oder auch auf Weisung des Verantwortlichen, ist der Auftragsverarbeiter dazu verpflichtet, alle im Zuge der Auftragsverarbeitung an ihn übermittelten bzw. von ihm verarbeiteten Daten, inkl. sämtlicher Vervielfältigungen, an den Verantwortlichen zurückzugeben und danach nachweislich, unwiederbringlich und vollständig, gemäß EUDSGVO, zu vernichten. Dies gilt auch für alle im Rahmen der Auftragsverarbeitung eingesetzten Subauftragnehmer. Der Nachweis der Vernichtung ist dem Verantwortlichen unaufgefordert zu übermitteln.

Liegt nachweislich ein schwerwiegender Verstoß gegen die aktuellen Datenschutzgesetze oder die Regelungen dieser Vereinbarungen durch den Auftragsverarbeiter oder einen Subauftragnehmer vor, so ist der Verantwortliche jederzeit dazu berechtigt, die Auftragsverarbeitervereinbarung außerordentlich und fristlos zu kündigen. Als schwerwiegender Verstoß gelten auch die erhebliche nicht Einhaltung der vereinbarten technischen und organisatorischen Maßnahmen oder die Weigerung zur Erfüllung einer Weisung ohne triftigen Grund. Bei lediglich unerheblichen Verstößen ist der Verantwortliche verpflichtet, dem Auftragsverarbeiter, oder einem eventuellen Subauftragnehmer, eine angemessene Frist zur Behebung zu setzen. Wird die Behebung nicht fristgerecht ausgeführt, so ist der Verantwortliche zur außerordentlichen und fristlosen Kündigung berechtigt. Sollten aus einer außerordentlichen Kündigung dem Verantwortlichen nachweislich Kosten entstehen, so ist der Auftragsverarbeiter verpflichtet, diese Kosten zu ersetzen.

7 Haftung

Der Auftragsverarbeiter haftet für Schäden, die auf Grund einer unzulässigen oder fehlerhaften Handlung oder durch einen Verstoß gegen aktuell gültige Datenschutzgesetze bzw. gegen Regelungen dieser Vereinbarung durch Mitarbeiter des Auftragsverarbeiters oder seiner Subauftragnehmer, entstanden sind gegenüber dem Verantwortlichen in vollem Umfang, sofern der Schaden nicht durch eine erteilte Weisung des Verantwortlichen entstanden ist. Die Beweislast, dass ein Schaden nicht durch sein Verschulden entstanden ist, liegt beim Auftragsverarbeiter. Bis zur Erbringung eines solchen Beweises ist der Verantwortliche durch den Auftragsverarbeiter von sämtlichen an ihn gestellten Ansprüchen freizuhalten.

Für einen Verstoß des Auftragsverarbeiters oder seiner Subauftragnehmer gegen die Regeln dieser Vereinbarung wird eine verschuldensunabhängige Vertragsstrafe von € 5.000,- je Fall vereinbart. Im Falle von anhaltenden Verstößen gilt jeder Kalendermonat als Einzelfall. Die Einrede des Fortsetzungszusammenhangs ist ausgeschlossen. Die Vertragsstrafe ist von anderen Ansprüchen des Verantwortlichen befreit.

8 Sonstiges

Sämtliche im Rahmen dieser Vereinbarung und der Auftragsverarbeitung erlangten Informationen und Daten sind, auch über die Beendigung der Auftragsverarbeitung hinaus, von beiden Parteien gegenüber Dritten vertraulich und Streng geheim zu halten, außer eine Bekanntgabe ist im Zuge dieser Vereinbarung genehmigt. Im Zweifel gilt strengste Geheimhaltung.

Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

Nebenabreden sind unzulässig. Sollten Nebenabreden vereinbart werden, so ist die Schriftform verpflichtend.

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht. In diesem Fall wird vereinbart, die Regelung zum Einsatz zu bringen, die der ursprünglichen Regelung am Nächsten kommt.

Auf diese Vereinbarung kommt österreichisches Recht zur Anwendung. Gerichtsstand ist

Unterschriften

Ort, Datum	Ort, Datum
Auftraggeber	Auftragnehmer

Anlage 1 – technische und organisatorische Maßnahmen

Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragnehmer mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen.

Für die Vernichtung gem. DIN 66399 gilt Schutzklasse 1.

1. Organisation der Informationssicherheit
2. Personalsicherheit
3. Verwaltung der Werte
4. Zugangssteuerung
5. Kryptographie
6. Physische und umgebungsbezogene Sicherheit
7. Betriebssicherheit
8. Kommunikationssicherheit
9. Anschaffung, Entwicklung und Instandhaltung von Systemen
10. Lieferantenbeziehungen
11. Handhabung von Informationssicherheitsvorfällen
12. Informationssicherheitsaspekte beim Business Continuity Management
13. Compliance

Anlage 2 – Zugelassene Subdienstleister

Anlage 3 – Weisungsberechtige Personen

Folgende Personen sind zur Erteilung und Entgegennahme von Weisungen befugt:

9 Schlussbemerkungen

Diese Vorlage dient der Unterstützung bei der Erreichung einer ausreichenden Datenschutzkonformität und erhebt keinen Anspruch auf Vollständigkeit. Auch ist die Erreichung einer 100%igen Datenschutzkonformität nicht möglich. Letztendlich bleibt ein gewisses Restrisiko. Die Höhe dieses Restrisikos unterliegt der Bereitschaft, wirtschaftliche und personelle Ressourcen zu investieren und ist im Endeffekt eine Entscheidung der Geschäftsleitung.

Die Neuheit der Regelungen aus der EUDSGVO und die Tatsache, dass sie erst am 25.5.2018 in nationales Recht übergehen, lässt den Schluss zu, dass noch keine Judikaturen aus der Praxis existieren und in Zukunft noch einige Aspekte von Gerichten und Behörden präzisiert werden.

Daher stellen die Angaben in diesem Leitfaden keine (rechts)verbindlichen Informationen dar, sondern spiegeln nur den aktuellen Wissens- und Erfahrungsstand wieder. Die Vorlage wird anhand von zukünftigen Entwicklungen kontinuierlich einer Überprüfung und Aktualisierung unterzogen, um Neuentwicklungen und zukünftige Rechtsprechungen ergänzen zu können.

Diese Vorlage ist keine abschließende Handlungsanweisung oder Rechtsberatung, d.h. eine Evaluierung konkreter Praxisfälle kann durch dieses Dokument nicht ersetzt werden.