VEREINBARUNG

über die Beauftragung mit der Datenverarbeitung gemäß Artikel 28 DSGVO

zwischen

WIEN ENERGIE GmbH
Thomas-Klestil-Platz 14
1030 Wien

in weiterer Folge "**Verantwortlicher**"

und

"**Auftragsverarbeiter**"

Präambel

Der Verantwortliche beauftragt den Auftragsverarbeiter mit der Erbringung von Lieferungen bzw. Leistungen (in der Folge "**zugrundeliegender Vertrag**"). Insoweit der Auftragsverarbeiter im Rahmen der Erfüllung des zugrundeliegenden Vertrags personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet und somit die Definition des Auftragsverarbeiters gemäß Artikel 4 Ziffer 8 DSGVO erfüllt, schließen die Parteien die gegenständliche Vereinbarung. Sie stellt einen integrierenden Bestandteil des zugrundeliegenden Vertrags dar, wobei sie diesem im Fall von Widersprüchen vorgeht. Den Parteien ist es unbenommen, vor oder nach Abschluss dieses Auftragsverarbeitervertrags einen spezielleren Auftragsverarbeitervertrag abzuschließen, der diesem Auftragsverarbeitervertrag dann vorgeht.

1. Beschreibung der beauftragten Datenverarbeitung

1.1. Die Dauer und der Gegenstand sowie die Art und der Zweck der Datenverarbeitung ergeben sich aus dem im zugrundeliegenden Vertrag vereinbarten zivilrechtlichen Grundgeschäft. Die Art der verarbeiteten personenbezogenen Daten und die Kategorien der davon betroffenen Personen sind ebenfalls dem zugrundeliegenden Vertrag und gegebenenfalls den bezughabenden Einträgen im Verarbeitungsverzeichnis zu entnehmen.

1.2. Falls der Verantwortliche hinsichtlich der beauftragten Datenverarbeitung gemeinsam verantwortlich mit der Wien Energie Vertrieb GmbH & Co KG („WEV“) iSd Artikel 26 DSGVO ist, schließt der Verantwortliche diese Vereinbarung auch im Namen der WEV ab, wodurch ebenso die WEV durch die Bestimmungen in dieser Vereinbarung berechtigt und verpflichtet wird.

Falls der Verantwortliche hinsichtlich der beauftragten Datenverarbeitung als Auftragsverarbeiter für die Wien Energie Vertrieb GmbH & Co KG tätig wird, gelten die Bestimmungen dieser Vereinbarung auch in Entsprechung der Verpflichtung nach Artikel 28 Abs 4 DSGVO zwischen den Parteien dieser Vereinbarung als vereinbart, wobei der Auftragsverarbeiter diesfalls als Sub-Auftragsverarbeiter für die Wien Energie Vertrieb GmbH & Co KG tätig wird.

2. Pflichten bei der Ausführung der beauftragten Datenverarbeitung

Bei der Ausführung der beauftragten Datenverarbeitung gelten für den Auftragsverarbeiter die folgenden Pflichten:

2.1. Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten ausschließlich zu den vom Verantwortlichen vorgegebenen Zwecken. Eine Verarbeitung der Daten für eigene Zwecke des Auftragsverarbeiters, einschließlich statistischer Auswertungen personenbezogener oder nicht personenbezogener Art, bedarf einer ausdrücklichen schriftlichen Genehmigung durch den Verantwortlichen.

2.2. Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation –, sofern er nicht durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

2.3. Die Ausführung der beauftragten Datenverarbeitung einschließlich der Datenspeicherung darf ausschließlich in einem Mitgliedstaat der Europäischen Union oder einem sonstigen Vertragsstaat des Europäischen Wirtschaftsraums erfolgen. Jede Übermittlung in ein oder Verarbeitung in einem Drittland bedarf der vorherigen schriftlichen Genehmigung des Verantwortlichen und darf überdies nur unter Einhaltung der besonderen Voraussetzungen von Kapitel V DSGVO erfolgen. Soll die Datenübermittlung durch den Auftragsverarbeiter vorbehaltlich geeigneter Garantien gemäß Artikel 46 DSGVO wie insbesondere im Rahmen von verbindlichen Verhaltensvorschriften (Artikel 46 Abs 2 lit b DSGVO), Standarddatenschutzklauseln (Artikel 46 Abs 2 lit c bzw d DSGVO) oder genehmigten Verhaltensregeln (Art 46 Abs 2 lit e DSGVO) erfolgen, hat der Auftragsverarbeiter dem Verantwortlichen auf dessen Aufforderung die diesbezüglichen Verträge bzw sonstige bezughabende Unterlagen wie beispielsweise eine durchgeführte Folgenabschätzung ("Transfer Impact Assessment") und eine Auflistung etwaiger getroffener zusätzlicher Maßnahmen zu übermitteln.

2.4. Der Auftragsverarbeiter leistet Gewähr, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen vor Aufnahme der Verarbeitungstätigkeit zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Diese Vertraulichkeits- bzw. Verschwiegenheitspflicht der zur Verarbeitung befugten Personen muss auch nach Beendigung ihrer Tätigkeit und Ausscheiden vom Auftragsverarbeiter aufrecht bleiben.

2.5. Der Auftragsverarbeiter ergreift alle gemäß Artikel 32 DSGVO erforderlichen Maßnahmen, um ein dem Risiko für die Rechte und Freiheiten natürlicher Personen angemessenes Schutzniveau zu gewährleisten. Die in Anlage 1 gelisteten Mindestanforderungen an erforderlichen Maßnahmen gelten als vereinbart und der Auftragsverarbeiter verpflichtet sich, diese einzuhalten. Für den Fall, dass der Auftragsverarbeiter diese Mindestanforderungen nicht erfüllen kann, ist er dazu verpflichtet, den Verantwortlichen schriftlich darüber zu informieren.

2.6. Der Auftragsverarbeiter darf einen weiteren Auftragsverarbeiter ("**Sub-Auftragsverarbeiter**") nur dann in Anspruch nehmen, wenn der Verantwortliche dies im Vorhinein gesondert schriftlich genehmigt hat.

2.7. Nimmt der Auftragsverarbeiter im Sinne des Punktes 2.6. dieser Vereinbarung die Dienste eines Sub-Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so hat er dem Sub-Auftragsverarbeiter im Wege eines schriftlichen Vertrags dieselben Datenschutzpflichten aufzuerlegen, die in dieser Vereinbarung zwischen dem Verantwortlichen und dem Auftragsverarbeiter festgelegt sind. Dabei müssen hinreichende Garantien dafür geboten werden, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

2.8. Der Auftragsverarbeiter unterstützt den Verantwortlichen angesichts der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte der betroffenen Person nachzukommen.

2.9. Der Auftragsverarbeiter unterstützt unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten.

2.10. Der Auftragsverarbeiter hat nach Abschluss der Erbringung der Datenverarbeitung alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder zu löschen oder zurückzugeben, sofern nicht nach dem Recht der Europäischen Union oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

2.11. Der Auftragsverarbeiter wird dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in dieser Vereinbarung niedergelegten Pflichten zur Verfügung stellen und Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglichen und dazu beitragen.

2.12. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzbestimmungen der Europäischen Union oder der Mitgliedstaaten verstößt.

Anlage 1

Mindestanforderungen an erforderlichen Maßnahmen im Sinne des Artikel 32 DSGVO:

Anforderung	Anforderungskriterien
Es liegt eine aktuell gültige Informationssicherheitsrichtlinie (bzw. IT-Sicherheitsrichtlinie) für das Unternehmen des Auftragsverarbeiters vor.	Die Informationssicherheitsrichtlinie muss die wesentlichen Anforderungen an Informationssicherheit und Datenschutz abdecken (alle Kernthemen müssen - sofern sie anwendbar sind - in dieser Richtlinie beschrieben werden) und sollte auf ein bestehendes Regelwerk aufbauen Die Richtlinie muss von der Geschäftsführung freigegeben und für Mitarbeiter verfügbar sein.
Mitarbeiter des Auftragsverarbeiters werden regelmäßig hinsichtlich IT-Sicherheit und Datenschutz geschult.	Die Schulung muss die Inhalte der Informationssicherheitsrichtlinie umfassen und auf aktuelle Bedrohungen eingehen. Die Inhalte müssen zumindest folgende Themen umfassen: - Sicherer Umgang mit Computern und Informationen (inkl. Datenschutz) - Passwörter richtig auswählen und verwalten-Sicher im Internet-E-Mails, Spam und Phishing-Gefährliche Schadprogramme - Verhalten und Vorgehen bei Verdacht auf IT-Sicherheitsvorfall Eine vollständige Schulung muss zumindest beim Eintritt stattfinden und aktualisierte Information muss zumindest alle zwei Jahre kommuniziert werden.
Im Unternehmen des Auftragsverarbeiters gibt es eine oder mehrere Personen, die für das Thema Informationssicherheit und Datenschutz zuständig sind.	Es muss zumindest eine namentlich benannte Person geben, die für das Thema Informationssicherheit & Datenschutz zuständig ist, d.h. sich um die Umsetzung der Maßnahmen kümmert und dafür die notwendige Zeit zur Verfügung gestellt bekommt. Diese Person muss das notwendige fachliche Grundwissen zu den Themen haben. Diese Tätigkeit kann neben anderen Tätigkeiten ausgeübt werden oder auch von Externen im Auftrag des Unternehmens wahrgenommen werden.
Das Verzeichnis aller Verarbeitungstätigkeiten (außer Art 30 Abs. 5 DSGVO ist einschlägig), IT-Systeme und Datenverarbeitungsprozesse samt den damit verbundenen Verantwortlichkeiten des Auftragsverarbeiters werden regelmäßig gepflegt.	Es muss ein Verzeichnis aller Verarbeitungstätigkeiten, der verwendeten IT-Systeme und aller Datenverarbeitungsprozesse geben. Dieses Verzeichnis muss zumindest den Namen des Systems enthalten und den dafür Verantwortlichen.
Der Zugang zu Systemen des Auftragsverarbeiters werden nach einem Berechtigungskonzept verwaltet, das jedem nur die für seine Arbeit notwenigen Rechte einräumt.	Sowohl der Zugang zu den Anwendungen als auch zu den Dateisystemen muss reglementiert sein und über korrekt gesetzte Berechtigungen sichergestellt werden, damit nur die Personen zugreifen können, die aufgrund ihres Jobprofils einen Bedarf dafür haben.

Von Mitarbeitern des Auftragsverarbeiters werden für alle Anwendungen Passwörter mit einer sicheren Mindeststärke verwendet.	Es muss klar beschriebene Mindestkriterien für Passwörter geben. Dort, wo es notwendig ist, ist Multi-Faktoren-Authentifizierung einzusetzen.
Der Auftragsverarbeiter aktualisiert all seine IT-Systeme und Anwendungen regelmäßig mit Sicherheitsupdates.	Regelmäßige Aktualisierung der Systeme mit Updates, die vom Hersteller zur Verfügung gestellt werden. Systeme, die nicht mehr vom Hersteller mit Sicherheitsupdates versorgt werden, werden rechtzeitig außer Betrieb genommen.
Der Auftragsverarbeiter überwacht seine IT-Systeme auf Malware und IT-Sicherheitsvorfälle.	Es muss zumindest eine aktuelle Antivirussoftware im Einsatz sein, welche laufend die Systeme und Dateien auf Schadsoftware überprüft. Im Verdachtsfall erfolgt eine Alarmierung im Unternehmen.
Der Auftragsverarbeiter verschlüsselt besondere Kategorien personenbezogener Daten iSd DSGVO im Falle einer Übertragung im Internet.	Es muss die Möglichkeit bestehen, Dateien verschlüsselt zu übertragen, entweder per E-Mail (z.B. S/MIME oder PDF verschlüsselt) oder per verschlüsseltem Upload.
Der Auftragsverarbeiter protokolliert die Nutzung seiner IT-Systeme, um Malware und IT-Sicherheitsvorfälle nachvollziehbar zu machen.	Es müssen zumindest die Standardprotokolle der Betriebssysteme aktiviert sein. Die Protokolle müssen dem Unternehmen zur Verfügung stehen. Es existiert eine Übersicht aller aktiven Systemprotokolle und deren Speicherort. Die Protokolle werden zumindest drei Monate aufbewahrt.
Der Auftragsverarbeiter hat einen Notfallplan, anhand dessen er auf einen IT-Sicherheitsvorfall bzw. auf einen Data Breach Verdachtsfall reagiert.	Der Auftragsverarbeiter muss organisatorisch in der Lage sein, den Verantwortlichen über Sicherheitsvorfälle oder Data Breach Verdachtsfälle unverzüglich zu informieren und entsprechend bei deren Abwicklung zu unterstützen.