

## Vereinbarung über eine Auftragsverarbeitung nach Art 28 DSGVO

Diese Vereinbarung wird abgeschlossen zwischen:

Dem Verantwortlichen:

**Gemeinde Altaussee  
Fischerndorf 61  
8992 Altaussee**

(im Folgenden Auftraggeber)

Dem Auftragsverarbeiter:

**IT-Kommunal GmbH  
Pius Parsch Platz 9/14  
1210 Wien**

(im Folgenden Auftragnehmer)

### 1. Gegenstand und Zweck der Vereinbarung

- (1) Gegenstand dieser Vereinbarung ist eine bereits bestehende Nutzungsvereinbarung zwischen dem Auftraggeber und dem Auftragnehmer über den Betrieb und die Bereitstellung von kommunalspezifischen Online-Formularen für den Auftraggeber sowie einem oder mehreren dem Auftraggeber zugeordneten Antragspostfächern, in welchen die von Antragstellern ausgefüllten Online-Anträge hinterlegt werden. Zweck der gegenständlichen Vereinbarung ist eine datenschutzrechtliche Präzisierung und Ergänzung der bestehenden Nutzungsvereinbarung, ohne dass sich an den eigentlichen Rahmenbedingungen (Leistungsumfang, Entgelt etc.) derselben Änderungen ergeben.

Die Online-Formulare dienen der Erfassung von – teils personenbezogenen – Daten, welche vom Auftraggeber

- a. für die Abwicklung von behördlichen Verfahren (im Bereich der Hoheitsverwaltung, z.B. Anträge gem. der jeweiligen Bauordnung);
- b. für die Abwicklung vorvertraglicher oder vertraglicher Aufgaben (im Bereich der Privatwirtschaftsverwaltung wie z.B. die Bestellung von Tickets für eine kommunale Kulturveranstaltung, im Bereich der internen Verwaltung, z.B. formularbasierte Urlaubsantragstellung);

- c. für die Abwicklung von Maßnahmen in öffentlichem Interesse (z.B. Meldung von Schäden an öffentlicher Infrastruktur – Bürgermeldungen);
- d. für die Verarbeitung von Daten zur Wahrung berechtigter Interessen des Auftraggebers oder eines Dritten, die gegenüber Schutzinteressen der von der Verarbeitung ihrer personenbezogenen Daten Betroffenen überwiegen (z.B. Anträge auf kommunale Förderungen).

(2) Je nachdem welche Online-Formulare aus dem vom Auftragnehmer bereitgestellten Pool vom Auftraggeber verwendet werden, werden folgende Datenkategorien verarbeitet:

- a. Angaben zum/zur Antragsteller/in – Natürliche Person
- b. Adresse des/der Antragstellers/in
- c. Angaben zum Hauptwohnsitz des/der Antragstellers/in
- d. Angaben zum Nebenwohnsitz des/der Antragstellers/in
- e. Zustelladresse
- f. Kontaktdaten des/der Antragstellers/in
- g. Urkundendaten zur Eheschließung
- h. Urkundendaten zur Geburt
- i. Angaben zum/zu Kind/Kindern des/der Antragstellers/in
- j. Adressdaten des/der Kindes/Kinder
- k. Angaben zum/zur Erziehungsberechtigten des/der Kindes/Kinder
- l. Führerscheindaten des/der Antragstellers/in
- m. Bankverbindungsdaten des/der Antragstellers/in
- n. Identitätsnachweis des/der Antragstellers/in
- o. Staatsbürgerschaftsnachweis des/der Antragstellers/in
- p. Nachweis früherer Namen des/der Antragstellers/in
- q. Angaben zur Verwendung der Strafregisterbescheinigung
- r. Angaben zur Wahlberechtigung
- s. Anknüpfungspunkt des/der Antragstellers/in zu Österreich
- t. Angaben zur Liegenschaft des/der Antragstellers/in
- u. Angaben zum Kraftfahrzeug/Anhänger des Antragstellers/in
- v. Berufliche Qualifikationen des/der Antragstellers/in
- w. Angaben zur Pflegegeldstufe
- x. Angaben zum Austritt aus Kirche oder Religionsgemeinschaft (Bekenntnis)
- y. Angaben zu Dienstgeber und Einkommen des/der Antragstellers/in
- z. Angaben zu künftigen Mitbewohnern des/der Antragstellers/in
- aa. Derzeitige Wohnverhältnisse des/der Antragstellers/in

(3) Folgende Kategorien betroffener Personen unterliegen der Verarbeitung:

- a. Gemeindebürgerinnen und -bürger (Einwohner)
- b. Eigentümerinnen und Eigentümer von Liegenschaften im Gemeindegebiet
- c. Personen, welche in einem Vertragsverhältnis oder sonstiger geschäftlicher oder behördlicher (gesetzlich determinierter) Verbindung mit der Gemeinde stehen
- d. Gäste (im Sinne von Touristen)
- e. Beschäftigte des Auftraggebers

- f. Sonstige Personen, welche mit dem Auftraggeber formularbasiert in Kontakt treten möchten

## 2. Dauer der Vereinbarung

Die Vereinbarung ist auf unbestimmte Zeit geschlossen und kann von beiden Parteien mit einer Frist von drei Monaten zum Abschlussdatum der an diese Vereinbarung geknüpfte Nutzungsvereinbarung des Online-Formularservices des Auftragnehmers gekündigt werden.

Die Möglichkeit zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

## 3. Pflichten des Auftragnehmers

- (1) Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge des Auftraggebers zu verarbeiten. Erhält der Auftragnehmer einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er - sofern gesetzlich zulässig - den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen. Desgleichen bedarf eine Verarbeitung der Daten für eigene Zwecke des Auftragnehmers eines schriftlichen Auftrages.
- (2) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Mitarbeiter und Mitarbeiterinnen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.
- (3) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat (Einzelheiten sind der Anlage ./1 zu entnehmen).
- (4) Der Auftragnehmer ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Rechte der betroffenen Person nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen. Wird ein entsprechender Antrag an den Auftragnehmer gerichtet und lässt dieser erkennen, dass der Antragsteller bzw. Antragsstellerin ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenanwendung hält, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller bzw. Antragsstellerin mitzuteilen.
- (5) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation).
- (6) Der Auftragnehmer führt für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO.
- (7) Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle, auch durch ihn beauftragte Dritte, eingeräumt. Der

Auftragnehmer verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.

- (8) Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben bzw. in dessen Auftrag zu vernichten. Ein Auftrag zur Vernichtung ist durch den Auftraggeber schriftlich zu erteilen. Für den Fall einer gewünschten Übergabe der Daten erfolgt diese über die dem Auftraggeber standardmäßig zur Verfügung gestellten Schnittstellen zur Datenabholung. Eine darüber hinaus gehende Datenübergabe in speziellen vom Auftraggeber gewünschten Formaten erfolgt ausschließlich auf Grundlage einer Aufwandsschätzung seitens des Auftragnehmers und gesonderten Beauftragung durch den Auftraggeber.
- (9) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

#### 4. Ort der Durchführung der Datenverarbeitung

Alle Datenverarbeitungstätigkeiten werden ausschließlich innerhalb der EU bzw. des EWR durchgeführt.

#### 5. Sub-Auftragsverarbeiter

Der Auftragnehmer ist befugt folgende Unternehmen als Sub-Auftragsverarbeiter hinzuziehen:

- Firma IPAX OG - Internet- und Marketing- Dienstleistungen, Barowitzkagasse 10/2/2/11, 1190 Wien  
*(Rechenzentrumsdienstleister der IT-Kommunal GmbH)*
- sendhybrid ÖPBD GmbH, Beratungs- und Kommunikationsunternehmen  
Göstinger Straße 213, 8051 Graz  
*(Partner der IT-Kommunal GmbH in der Bereitstellung der „E-Box“ als Antragsdatenpostfach)*
- Bernhard Zangl, Freelance Business Intelligence Consultant & Software Developer, am Kaisermühlendamm 107/3/340, 1220 Wien  
*(Auftragnehmer der IT-Kommunal im Bereich IT-Entwicklung und Support)*

Der Auftragnehmer schließt die erforderlichen Vereinbarungen im Sinne des Art 28 Abs 4 DSGVO mit dem Sub-Auftragsverarbeiter ab, sofern die - diesem übertragenen - Aufgaben und Tätigkeiten eine datenschutzrechtliche Relevanz ergeben. Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Auftragnehmer auf Grund dieser Vereinbarung obliegen. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der

Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

Änderungen eines Sub-Auftragsverarbeiters sind unter Einhaltung der eingangs genannten Voraussetzungen für Vereinbarungen mit Sub-Auftragsverarbeitern zulässig.

Wien, am 05.06.2018

Für den Auftragnehmer:

IT-Kommunal	Unterzeichner	IT-Kommunal GmbH
	Datum/Zeit-UTC	2018-06-06T13:15:41+02:00
	Aussteller-Zertifikat	GLOBALTRUST ADVANCED 1
	Serien-Nr.	144500562040267203529839677018
Prüfinformation	Informationen zur Prüfung der elektronischen Signatur finden Sie unter: <a href="https://www.signaturpruefung.gv.at">https://www.signaturpruefung.gv.at</a>	
Hinweis	Das für die Erstellung der Signatur verwendete Zertifikat ist ausschließlich dem Signator zugeordnet und erlaubt eine Feststellung von nachträglichen Veränderungen der Daten, auf die sie sich bezieht.	

Für den Auftraggeber:

Der Bürgermeister



GERALD LOTZ

[Name samt Funktion]

ALTAUSSEE, 7.6.2018

[Ort, Datum]

## Anlage ./1 - Konsolidierte Technische und Organisatorische Maßnahmen gemäß Art. 32 DSGVO

Bei den nachfolgenden technischen und organisatorischen Maßnahmen handelt es sich um Mindeststandards, die vom Auftragnehmer bez. den in Frage kommenden Subauftragnehmern eingehalten werden.

**Hinweis:** Nicht auf jeden der gelisteten Subauftragnehmer treffen alle angeführten technischen und organisatorischen Maßnahmen zu.

### Vertraulichkeit

- **Zutrittskontrolle:** Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen, z.B.: Schlüssel, Magnet- oder Chipkarten, elektrische Türöffner, Portier, Sicherheitspersonal, Alarmanlagen, Videoanlagen;
- **Zugangskontrolle:** Schutz vor unbefugter Systembenutzung, z.B.: Kennwörter (einschließlich entsprechender Policy), automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
- **Zugriffskontrolle:** Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Standard-Berechtigungsprofile auf „need to know-Basis“, Standardprozess für Berechtigungsvergabe, Protokollierung von Zugriffen, periodische Überprüfung der vergebenen Berechtigungen, insb von administrativen Benutzerkonten;
- **Pseudonymisierung:** Eine Pseudonymisierung ist bei der Datenanwendung „amtsweg.gv.at“ nicht möglich.
- **Klassifikationsschema für Daten:** Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).

### Integrität

- **Weitergabekontrolle:** Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;
- **Eingabekontrolle:** Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

### Verfügbarkeit und Belastbarkeit

- **Verfügbarkeitskontrolle:** Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV, Dieselaggregat), Virenschutz, Firewall, Meldewege und Notfallpläne, Security Checks auf Infrastruktur- und Applikationsebene, mehrstufiges Sicherheitskonzept mit verschlüsselter Auslagerung der Sicherungen in ein Ausweichrechenzentrum, Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern bzw. Mitarbeiterinnen;

- Rasche **Wiederherstellbarkeit**;
- **Löschungsfristen**: Der Auftraggeber hat die uneingeschränkte Möglichkeit, sämtliche, in den ihm vom Auftragnehmer zur Verfügung gestellten Antragsdatenpostfächern hinterlegten Anträge, welche u.a. auch personenbezogene Daten beinhalten, zu löschen. Die Einhaltung von gesetzlich vorgeschriebenen oder durch andere Regelungen festgelegten Löschrufen obliegt allein dem Auftraggeber.

## Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- **Datenschutz-Management**, einschließlich regelmäßiger Mitarbeiter-Schulungen;
- **Incident-Response-Management**
- **Datenschutzfreundliche Voreinstellungen**
- **Auftragskontrolle**: Keine Auftragsdatenverarbeitung im Sinne von Art 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Auftragsverarbeiters (ISO-Zertifizierung, ISMS), Vorabüberzeugungspflicht, Nachkontrollen.