gemdat

# Auftragsbearbeitungsvereinbarung
(ABV)

**zu den Betriebsdienstleistungen.**

Diese Auftragsbearbeitungsvereinbarung ist ein integrierter Bestandteil zu den von der Gemdat AG ausgestellten Betriebsverträgen.

# 1 Gegenstand dieser Vereinbarung

Diese Auftragsbearbeitungsvereinbarung **(Vereinbarung)** regelt die Pflichten und Zuständigkeitsbereiche der Parteien in Bezug auf die Auftragsbearbeitung durch Leistungserbringerin für die Leistungsbezügerin.

# 2 Verhältnis zum Hauptteil des Vertrags

Diese Vereinbarung untersteht den Bestimmungen des Betriebs- und Wartungsvertrags zwischen den Parteien **(Vertrag)** und ist integraler Bestandteil desselben.
Die Bestimmungen dieser Vereinbarung schränken die Rechte und Pflichten der Parteien in Bezug auf die Bereitstellung bzw. die Nutzung der Software unter dem Vertrag nicht ein. Ihren Regelungsgegenstand betreffend gehen die Bestimmungen dieser Vereinbarung indes den Bestimmungen des Hauptteil des Vertrags vor.

# 3 Angaben zur Auftragsbearbeitung

Gegenstand und Zweck der Bearbeitung ist die Bereitstellung der Software gemäss Vertrag zur Nutzung durch die Leistungsbezügerin gemäss Bestimmungen des Vertrags.
Folgende Personendatenarten/-kategorien ("vertragsgegenständliche Personendaten") werden bearbeitet:

— Personenstammdaten
— Kommunikationsdaten (z.B. Telefon, E-Mail)
— Objektdaten (Daten zu Gebäuden, Grundstücken und Eigentumsbeziehungen)
— Baugesuchsdaten
— Baugesuchsdokumente
— Verfügungen und Schreiben zu Baugesuchen und Kontrollen
— Abrechnungen zu Baugesuchen und Kontrollen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

— Eigentümer von Grundstücken
— Beteiligte Personen an Baugesuchen
— Behörden und Fachstellen
— Daten von Fachfirmen

# 4 Weisungsgebundenheit, Zweckbindung, Kontrolle

Die Leistungserbringerin verpflichtet sich und sichert zu, dass die Leistungserbringerin alle vertragsgegenständlichen Personendaten ausschliesslich zum in Ziffer 3 beschriebenen Zweck; in Übereinstimmung mit den Weisungen der Leistungsbezügerin; und in Übereinstimmung mit dieser Vereinbarung bearbeitet; und nicht für eigene Zwecke verwendet.

# 5 Technische und organisatorische Massnahmen

Die Leistungserbringerin verpflichtet sich, im Interesse der Vertraulichkeit, Integrität und vertragsgemässen Verfügbarkeit der vertragsgegenständlichen Personendaten angemessene technische und organisatorische Massnahmen zu treffen. Die Leistungserbringerin implementiert oder stellt hierzu Zugangskontrollen, Zugriffskontrollen sowie Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Massnahmen sicher.

Bei der Auswahl der Massnahmen berücksichtigt die Leistungserbringerin den Stand der Technik, die Implementierungskosten sowie die Art, den Umfang, die Umstände und die Zwecke der Bearbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für betroffene Personen.

Die technischen und organisatorischen Massnahmen, welche die Leistungserbringerin zum Schutz dieser Personendaten ergreift und gewährleistet, sind in **Beilage 1** festgehalten.

# 6 Informations- und Unterstützungspflichten

Die Leistungserbringerin verpflichtet sich, die Leistungsbezügerin unverzüglich und von sich aus zu informieren, wenn die Leistungserbringerin der Ansicht ist, dass die Leistungserbringerin nicht mehr in der Lage ist, den Pflichten gemäss dieser Vereinbarung nachzukommen; wenn ein unbeabsichtigter oder unbefugter Zugriff auf die vertragsgegenständlichen Personendaten oder eine andere Verletzung der Datensicherheit vorliegt (vgl. dazu Ziffer 8); oder über jede Anfrage zur Ausübung von Betroffenenrechten, die die Leistungserbringerin direkt von betroffenen Personen in Bezug auf vertragsgegenständliche Personendaten erhalten hat (vorausgesetzt, die Leistungserbringerin kann eine Zuordnung an die betroffene Person gestützt auf die Angaben der betroffenen Person vornehmen).

Die Leistungserbringerin verpflichtet sich, die Leistungsbezügerin auf Anfrage und gegen separate Vergütung bei der Beantwortung von Anfragen betroffener Personen zur Ausübung datenschutzrechtlicher Betroffenenrechte zu unterstützten.

Zudem verpflichtet sich die Leistungserbringerin, die Leistungsbezügerin auf Anfrage und gegen separate Vergütung bei Datenschutz-Folgenabschätzungen und vorherigen Konsultationen von Datenschutzaufsichtsbehörden zu unterstützen.

## 7 Geheimhaltung

Die Leistungserbringerin verpflichtet sich zur Geheimhaltung der vertragsgegenständlichen Personendaten und hat die mit der Auftragsbearbeitung betrauten Personen durch Vereinbarung zur Wahrung der Vertraulichkeit zu verpflichten.

Diese Geheimhaltungsverpflichtungen gelten auch nach Beendigung dieser Vereinbarung.

## 8 Verletzungen der Datensicherheit

Sofern die Leistungserbringerin von einem unbefugten oder rechtswidrigen Zugriff, einer unbefugten Bearbeitung oder Weitergabe von den vertragsgegenständlichen Personendaten ("Datensicherheits-Verletzung") im Rahmen dieser Vereinbarung Kenntnis erlangt, wird die Leistungserbringerin die Leistungsbezügerin so rasch als möglich benachrichtigen.

Die Leistungserbringerin verpflichtet sich ferner, Massnahmen zu ergreifen, um den Verstoss zu untersuchen und die Auswirkungen zu ermitteln, zu verhindern und in Absprache mit der Leistungsbezügerin die Wiederherstellung oder Massnahmen durchzuführen, die zur Behebung des Verstosses erforderlich sind.

Die Leistungsbezügerin ist ihrerseits verpflichtet, die Leistungserbringerin über von der Leistungsbezügerin festgestellte und vertragsgegenständliche Personendaten betreffende Datensicherheits-Verletzungen zu informieren.

## 9 Unter-Auftragsbearbeiter

Unter-Auftragsbearbeiter sind natürliche oder juristische Personen, die die Leistungserbringerin zur (Unter-) Auftragsbearbeitung beizieht. Die Leistungserbringerin ist berechtigt, Unter-Auftragsbearbeiter zur Bearbeitung der vertragsgegenständlichen Personendaten beizuziehen. Die Leistungserbringerin ist in solchen Fällen verpflichtet, mit Unter-Auftragsbearbeitern im erforderlichen Umfang eine Vereinbarung zu treffen, die der Leistungserbringerin die Einhaltung der Bestimmungen der vorliegenden Vereinbarung zwischen der Leistungserbringerin und der Leistungsbezügerin ermöglicht.

Die Leistungsbezügerin anerkennt, dass zum Zeitpunkt des Inkrafttretens dieser Vereinbarung die Infrastructure-as-a-Service-Anbieterin [Microsoft Ireland Operations Limited, Dublin] Unter-Auftragsbearbeiterin ist. Zudem werden Dienstleistungen im

Bereich technischem Support von der Firma Netrics [Netrics Biel AG, Biel] bezogen. Die Leistungserbringerin wird die Leistungsbezügerin vorab in geeigneter Weise informieren, wenn die Leistungserbringerin nach Inkrafttreten dieser Vereinbarung neue Unter-Auftragsbearbeiter beizieht oder bestehende austauscht. Wenn die Leistungsbezügerin dem nicht innerhalb von dreissig (30) Tagen nach dem Datum der Mitteilung aus wichtigen datenschutzrechtlichen Gründen widerspricht, gilt der neue oder ausgetauschte Unter-Auftragsbearbeiter als genehmigt.

## 10 Rückgabe oder Löschung vertragsgegenständlicher Personendaten bei Vertragsbeendigung

Nach Beendigung des Vertrags wird die Leistungserbringerin, sofern von der Leistungsbezügerin gewünscht, die gespeicherten vertragsgegenständlichen Personendaten herausgeben.

Die Leistungserbringerin wird gespeicherte vertragsgegenständliche Personendaten, die die Leistungsbezügerin nicht herausverlangt oder deren Herausgabe technisch nicht möglich ist, auf Anfrage der Leistungsbezügerin löschen.

Die Leistungserbringerin wird die gespeicherten Daten frühestens 30 Tage nach Herausgabe der Daten löschen. Erfolgt bis dahin keine Mitteilung der Leistungsbezügerin, dass die Daten nicht lesbar oder unvollständig seien, so ist die Leistungserbringerin zur vollständigen Löschung der Daten berechtigt. Wird durch die Leistungsbezügerin keine schriftliche Herausgabe der Daten verlangt, so ist die Leistungserbringerin berechtigt, die Daten 30 Tage nach Vertragsende zu löschen.

## 11 Laufzeit der Vereinbarung

Die Laufzeit dieser Vereinbarung entspricht der Dauer des Vertrags, sofern sich aus den Bestimmungen dieser Vereinbarung keine zeitlich darüber hinausgehenden Verpflichtungen ergeben. In Ansehung dieser Verpflichtungen besteht diese Vereinbarung solange fort, bis diese erloschen sind. Durch diese Regelung wird keine Modifizierung der im Vertrag vereinbarten Kündigungsrechte vorgenommen.

## 12 Änderungen der Vereinbarung

Die Leistungserbringerin ist berechtigt, diese Vereinbarung jederzeit abzuändern, wenn die Leistungserbringerin dies zur Anpassung an neue oder geänderte gesetzliche Bestimmungen oder regulatorische Vorschriften für notwendig erachtet, oder wenn solche Änderungen nicht zu einer Verschlechterung der allgemeinen Sicherheit der Auftragsbearbeitung für die Leistungsbezügerin gemäss dieser Vereinbarung führen und (im Ermessen der Leistungserbringerin) die Rechte der betroffenen Personen nicht negativ

beeinträchtigt werden. Wenn die Leistungsbezügerin die Leistungen aus dem Vertrag weiterhin nutzt, bedeutet dies, dass die Leistungsbezügerin den Änderungen zustimmt.

## 13 Audit

Die Leistungsbezügerin kann bei der Leistungserbringerin einmal jährlich Audits zur Prüfung der angemessenen technischen und organisatorischen Massnahmen, Sicherheitseinrichtungen oder der sonstigen Einhaltung dieser Vereinbarung durchführen oder durchführen lassen. Die Kosten dafür trägt die Leistungsbezügerin. Die Leistungserbringerin unterstützt die Audits im Rahmen eines verhältnismässigen Aufwands unentgeltlich.

Die Prüfungs- und Auditrechte gemäss dieser Ziffer 1213 gelten nur insoweit als der Vertrag der Leistungsbezügerin nicht anderweitig erlaubt, die Vertragserfüllung (einschliesslich der Pflichten gemäss dieser Vereinbarung) der Leistungserbringerin zu prüfen und zu auditieren.

# 14 Beilage 1: Technische und Organisatorische Massnahmen

## 14.1 Vertraulichkeit

| Massnahme | Umgesetzte Massnahmen |
|---|---|
| Zutrittskontrolle<br><br>Unbefugten ist der (räumliche) Zutritt zu Datenverarbeitungsanlagen, in denen personenbezogene Daten verarbeitet werden oder genutzt werden, zu verwehren. | Gemdat betreibt das Rechenzentrum nicht selbst. Die benötigte Rechenleistung wird von der Firma Microsoft bezogen. Das Azure-Rechenzentrum befindet sich in der Schweiz und ist ISO27001 zertifiziert. ISO27001 definiert gemäss A11.1.1-6 die einzuhaltenden Zutrittskontrollen. |
| Zugangskontrolle<br><br>Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. | Gemdat betreibt das Rechenzentrum nicht selbst. Die benötigte Rechenleistung wird von der Firma Microsoft bezogen. Das Azure-Rechenzentrum befindet sich in der Schweiz und ist ISO27001 zertifiziert. ISO27001 definiert gemäss A11.1.1-6 die einzuhaltenden Zugangskontrollen. |
| Zugriffskontrolle<br><br>Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungs-systems Berechtigten ausschliesslich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. | Folgende Zugriffskontrollen sind implementiert:<br>— Gemdat unterhält ein Berechtigungskonzept zur Sicherstellung der Zugriffsberechtigungen.<br>— Gemdat dokumentiert bei der letzten Datenänderungen pro Datensatz den Benutzer und den Mutationszeitpunkt in der Datenbank.<br>— Nur authentifizierte und durch Gemdat autorisierte User haben Zugang.<br>— Der Zugriff auf die Software erfolgt nur über persönliche Accounts |

| | |
|---|---|
| Trennungskontrolle<br><br>Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. | Folgende Trennungskontrollen sind implementiert:<br>— Pro Kunde wird eine eigene Installation, IIS, Windows Dienst und Datenbank betrieben. Dabei erfolgt der Zugriff auf die Daten über einem pro Installation einzigartigen Service Benutzer. Dieser ist als einziger Benutzer berechtigt Lese- und Schreibaufgaben direkt in der Datenbank durchzuführen. Dies auf allen Fachapplikationsdaten, wie Datenbank, Schnittstellen und Dokumente.<br>— Produktiv und Testsysteme werden getrennt voneinander betrieben. |

## 14.2 Integrität

| Massnahme | Umgesetzte Massnahmen |
|---|---|
| Weitergabekontrolle<br><br>Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. | Folgende Weitergabekontrollen sind implementiert:<br>— Schnittstellenaktivitäten werden in der Auftragskontrolle von «gemdat bau» protokolliert<br>— Für File-Schnittstellen stellt Gemdat einen Azure Share Sync. zur Verfügung. Die Daten werden bei der Übertragung mit TLS verschlüsselt<br>— Bei WebService-Schnittstellen werden die Daten verschlüsselt übertragen<br>— Die Daten werden «on rest» verschlüsselt gehalten.<br><br>Abgesehen von Schnittstellen findet keine Datenweitergabe ohne ausdrücklichen Auftrag durch die Leistungsbezügerin statt. |
| Eingabekontrolle<br><br>Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. | Folgende Eingabekontrollen sind implementiert:<br>— Gemdat dokumentiert bei der letzten Datenänderung pro Datensatz den Benutzer und den Mutationszeitpunkt in der Datenbank |

## 14.3 Verfügbarkeit und Belastbarkeit

| Massnahme | Umgesetzte Massnahmen |
|---|---|
| Verfügbarkeitskontrolle<br><br>Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige oder mutwillige Zerstörung oder Verlust geschützt sind. Rasche Wiederherstellbarkeit | Folgende Verfügbarkeitskontrollen sind implementiert:<br>— Gemdat unterhält ein Backupkonzept sowie ein Notfall Recovery Plan.<br>— Gemdat betreibt das Rechenzentrum nicht selbst, sondern kauft die benötigte Rechenleistung ein. Das beauftragte Rechenzentrum ist ISO27001:2013 zertifiziert<br>— Gemdat unterhält ein Service Monitoring. |