gemdat

Auftragsbearbeitungsvereinbarung (ABV)

zu den Betriebs- und SaaS-Dienstleistungen.

Diese Auftragsbearbeitungsvereinbarung ist ein integrierter Bestandteil zu den von der Gemdat AG ausgestellten Betriebs- und SaaS-verträgen.

1 Gegenstand dieser Vereinbarung

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

2 Verhältnis zum Hauptteil des Vertrags

Diese Vereinbarung untersteht den Bestimmungen des Betriebs- und Wartungsvertrag, SaaS-Vertrag oder ASP-Vertrags zwischen den Parteien **(Vertrag)** und ist integraler Bestandteil desselben.

3 Angaben zur Auftragsbearbeitung

Die Leistungserbringerin bearbeitet Personendaten im Auftrag der Leistungsbezügerin. Dies umfasst Tätigkeiten, die im Vertrag konkretisiert sind. Die Leistungsbezügerin ist im Rahmen des Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmässigkeit der Datenweitergabe an die Leistungserbringerin sowie für die Rechtmässigkeit der Datenverarbeitung allein verantwortlich.

Gegenstand und Zweck der Bearbeitung ist die Bereitstellung der Software gemäss Vertrag zur Nutzung durch die Leistungsbezügerin und/oder deren Kunden 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 Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung Löschung oder Auskunft an die Leistungserbringerin, wird die Leistungserbringerin die betroffene Person an die Leistungsbezügerin verweisen, sofern eine Zuordnung an die Leistungsbezügerin nach Angaben der betroffenen Person möglich ist. Die Leistungserbringerin leitet den Antrag der betroffenen Person unverzüglich an die Leistungsbezügerin weiter. Die Leistungserbringerin unterstützt die Leistungsbezügerin im Rahmen ihrer Möglichkeiten auf Weisung soweit vereinbart. Die Leistungserbringerin haftet nicht, wenn das Ersuchen der betroffenen Person von der Leistungsbezügerin nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

5 Weisungsgebundenheit, Zweckbindung, Kontrolle

Die Leistungserbringerin verpflichtet sich und sichert zu, dass sie alle Informationen / Daten wie Personen- und/oder Sachdaten etc., welche sie im Rahmen ihrer Tätigkeiten für die Leistungsbezügerin bearbeitet, ausschliesslich zum in Ziffer 3 vorstehend beschriebenen Zweck, unter Einhaltung der Weisungen der Leistungsbezügerin und in Übereinstimmung mit dieser Vereinbarung bearbeitet sowie, dass sie diese Daten nicht für eigene Zwecke verwendet.

6 Technische und organisatorische Massnahmen

Die Leistungserbringerin verpflichtet sich, zur Sicherstellung 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 die Schwere des Risikos datenschutzrechtlicher Verletzungen.

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

7 Informations- und Unterstützungspflichten

Die Leistungserbringerin verpflichtet sich, die Leistungsbezügerin unverzüglich und von sich aus zu informieren, wenn die Leistungserbringerin der Ansicht ist, dass sie nicht mehr

in der Lage ist, ihren Pflichten gemäss dieser Vereinbarung nachzukommen oder wenn ein unbeabsichtigter oder unbefugter Zugriff auf die vertragsgegenständlichen Personen- und oder Sachdaten oder eine andere Verletzung der Datensicherheit vorliegt (vgl. dazu Ziffer 9 nachstehend). Die Leistungserbringerin hat die Leistungsbezügerin zudem unverzüglich über jede Anfrage zur Ausübung von Betroffenenrechten zu unterrichten, die die Leistungserbringerin direkt von betroffenen Personen in Bezug auf vertragsgegenständliche Personendaten erhalten hat (vorausgesetzt, die Leistungserbringerin kann gestützt auf die Angaben der betroffenen Person eine Zuordnung zur 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.

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

8 Geheimhaltung

Die Leistungserbringerin verpflichtet sich zur Geheimhaltung aller Informationen aus dem Geschäftsbereich der Leistungsbezügerin, die weder offenkundig noch allgemein zugänglich sind, und hat alle von ihr mit der Auftragsbearbeitung betrauten Personen (Hilfspersonen und Unter-Auftragnehmer) mittels entsprechender Vereinbarung zur Wahrung der Vertraulichkeit zu verpflichten.

Diese Geheimhaltungsverpflichtungen sind schon vor Vertragsschluss zu wahren und gelten auch nach Beendigung dieser Vereinbarung weiter. Vorbehalten bleiben gesetzliche Aufklärungspflichten.

9 Verletzungen der Datensicherheit

Bei Kenntnisnahme von einem unbefugten oder rechtswidrigen Zugriff auf bzw. von einer unbefugten Bearbeitung oder Weitergabe von vertragsgegenständlichen Daten ("Datensicherheits-Verletzung") ist die Leistungserbringerin verpflichtet, die Leistungsbezügerin unverzüglich zu informieren (vgl. Ziffer 7 vorstehend) sowie Massnahmen zu ergreifen, um den Verstoss zu untersuchen und die Auswirkungen zu ermitteln, zu verhindern und in Absprache mit der Leistungsbezügerin Vorkehrungen zu treffen, die zur Behebung des Verstosses erforderlich sind.

10 Unter-Auftragnehmer

Unter-Auftragnehmer sind Dritte (natürliche oder juristische Personen), welche die Leistungserbringerin zur (Unter-) Auftragsbearbeitung beizieht. Die Leistungserbringerin ist berechtigt, Unter-Auftragnehmer zur Bearbeitung der vertragsgegenständlichen Personendaten beizuziehen. Die Leistungserbringerin ist in solchen Fällen verpflichtet, mit den Unter-Auftragnehmern eine Vereinbarung abzuschliessen, mit der die Einhaltung der Bestimmungen der vorliegenden Vereinbarung durch die Unter-Auftragnehmer sichergestellt wird.

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.

11 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.

12 Laufzeit der Vereinbarung

Die Laufzeit dieser Vereinbarung entspricht der Dauer des Vertrags, sofern sich aus den Bestimmungen dieser Vereinbarung keine zeitlich darüber hinaus gehenden

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.

13 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.

14 Audit und Kontrolle

Die Leistungsbezügerin kann bei der Leistungserbringerin einmal jährlich die Durchführung bzw. das Durchführenlassen von Audits zur Prüfung der Angemessenheit der technischen und organisatorischen Massnahmen, Sicherheitseinrichtungen oder der sonstigen Einhaltung dieser Vereinbarung verlangen. Die Kosten dafür trägt die Leistungsbezügerin. Die Leistungserbringerin unterstützt die Audits im Rahmen eines verhältnismässigen Aufwands unentgeltlich.

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

15 Beilage 1: Technische und Organisatorische Massnahmen

15.1 Vertraulichkeit

Massnahme	Umgesetzte Massnahmen
Zutrittskontrolle Unbefugten ist der (räumliche) Zutritt zu Datenverarbeitungsanlagen, in denen personenbezogene Daten verarbeitet werden oder genutzt werden, zu verwehren.	Die Leistungserbringerin 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 Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.	Die Leistungserbringerin 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 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: — Die Leistungserbringerin unterhält ein Berechtigungskonzept zur Sicherstellung der Zugriffsberechtigungen. — «gemdat bau» dokumentiert bei der letzten Datenänderungen pro Datensatz den Benutzer und den Mutationszeitpunkt in der Datenbank. — Nur authentifizierte und autorisierte User haben Zugang. — Der Zugriff auf die Software erfolgt nur über persönliche Accounts

Trennungskontrolle Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.	Folgende Trennungskontrollen sind implementiert: — Pro Leistungsbezügerin wird eine eigene Installation, IIS, Windows Dienst und Datenbank betrieben. Dabei erfolgt der Zugriff auf die Daten pro Installation über einen eigenen 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. — Produktiv und Testsysteme werden getrennt voneinander betrieben.

15.2 Integrität

Massnahme	Umgesetzte Massnahmen
Weitergabekontrolle 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: — Schnittstellenaktivitäten werden in der Auftragskontrolle von «gemdat bau» protokolliert — Für File-Schnittstellen stellt Gemdat einen Azure Share Sync. zur Verfügung. Die Daten werden bei der Übertragung mit TLS verschlüsselt — Bei WebService-Schnittstellen werden die Daten verschlüsselt übertragen Abgesehen von Schnittstellen findet keine Datenweitergabe ohne ausdrücklichen Auftrag durch die Leistungsbezügerin statt.
Eingabekontrolle 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: — «gemdat bau» dokumentiert bei der letzten Datenänderung pro Datensatz den Benutzer und den Mutationszeitpunkt in der Datenbank

15.3 Verfügbarkeit und Belastbarkeit

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