stowasserservice
Software | Schulung | Support

Auftragsverarbeitung gemäß Art. 28 DSGVO

Zwischen dem Kunden (Verantwortlicher) und der StowasserService GmbH & Co. KG (Auftragsverarbeiter), Hauptstraße 47f Radebeul, Sachsen 01445 wird nachfolgender Vertrag geschlossen (**Vertrag als PDF herunterladen**).

Präambel

Zwischen dem Verantwortlichen und dem Auftragsverarbeiter besteht ein Vertrag über die Nutzung der im entsprechenden Angebotsbestellprozess bezeichneten Softwareprodukte des Auftragsverarbeiters durch den Verantwortlichen. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Umsetzung eigener Geschäftszwecke in diesem Zusammenhang – eine Übertragung von ‚Funktionen' ist ausdrücklich nicht beabsichtigt.

1. Gegenstand und Dauer des Auftrags

1.1 Je nach Angebotsbestellprozess wurde ein Vertrag über die Nutzung einer oder mehrerer der nachfolgend genannten Softwareprodukte abgeschlossen. :

1.1.1. Zum Kern des Softwareprodukts PROGEMIS gehören folgende Funktionalitäten:

1. ein bestehendes Gewässernetz in Abschnitte zu organisieren, und dabei entsprechende Lage- und Zuständigkeitsinformationen, Bestandsinformationen zur Vegetation, Restriktionen, Zielen und Erfordernissen anzugeben,

2. Anlagen mit zugehörigen technischen Informationen, Lage und Zielen zu verwalten,

3. Maßnahmenerfordernisse (nicht in PROGEMIS BASIC) zur Erreichung der zuvor festgelegten Ziele in einem Basisplan zu verwalten, sowie

4 explizite Arbeitspläne für konkrete Bewirtschaftungsjahre aus den Maßnahmenerfordernissen, mit dann konkreten Durchführungszeiten und Zuständigkeiten abzuleiten.

1.1.2 Zum Kern des Softwareprodukts SOFIE gehören folgende Funktionalitäten:

1. Modul EVAT unterstützt bei der Eignungsermittlung ingenieurbiologischer Bauweisen. Es bietet eine strukturierte Entscheidungsunterstützung und Argumentationshilfe zur transparenten Auswahl geeigneter Bauweisen.

2. Modul ISYS ist ein Nachschlagewerk für ingenieurbiologische Bauweisen anhand von Steckbriefen, Regeldetails, Bauschritten, Pflegeschritten und Fotos.

3. Modul SITE zur interaktive Ermittlung der Fließgewässerlandschaft und potentiellen natürlichen Vegetation.

In der im Bestellprozess erworbenen Software kann es möglich sein, über die Funktionalität der "Bemerkungen und Anhänge" sowie "Kommentare" zusätzliche Dateien zur Dokumentation hochzuladen und mit Dritten zu teilen. Dabei trägt der Verantwortliche die volle Verantwortung für die hochgeladenen Dateien, deren Inhalt vom Auftragsverarbeiter nicht geprüft wird.

Der Gegenstand dieses Auftrags ergibt sich im Übrigen aus dem bestehenden Lizenzvertrag, auf den hier verwiesen wird. Dabei handelt es sich um die Verarbeitung personenbezogener Daten (im Weiteren „Daten“) durch den Auftragsverarbeiter für den Verantwortlichen im Zusammenhang mit der Nutzung der Software.

Neben der Erhebung, Verarbeitung und Nutzung von Daten im Auftrag als Hauptzweck werden u.a. personenbezogene Daten im Rahmen der Kunden-, Lieferanten- und Personalverwaltung sowie für sonstige Zwecke (z.B. Geschäftspartner- und Interessentenbetreuung, Hilfe und Support, Analyse und Verbesserung des Dienstleistungsangebots, sowie nach vorheriger Einwilligung für Marketingmaßnahmen) erhoben, verarbeitet oder genutzt.

1.2 Dauer der Vereinbarung

Die Laufzeit dieses Vertrages entspricht der Laufzeit des Lizenzvertrages.

2. Konkretisierung des Auftragsverhältnisses

2.1 Art und Zweck der vorgesehenen Verarbeitung von Daten

Der Zweck der Softwareprodukte ist es, Kommunen, Gemeinden, Gewässerunterhaltungsverbände oder auch spezialisierte Ingenieurbüros bei der

Durchführung ihrer Geschäftstätigkeit im Zusammenhang des Gewässermanagements optimal zu unterstützen und zu entlasten. Hierbei erbringen die Softwareprodukte insbesondere Leistungen der Datenverarbeitung sowie andere Dienstleistungen und Nebenleistungen. Der Auftragsverarbeiter erhält dabei Zugriff auf die bei der Benutzung der in den vertragsgegenständlichen Softwaremodulen gespeicherten personenbezogenen Daten und nutzt diese zum Zweck der Leistungserbringung und zu damit kompatiblen Zwecken unter den Voraussetzungen des Art. 6 Abs. 4 DSGVO im Auftrag des Auftraggebers. Der Umfang der vorgenommenen Erhebung, Verarbeitung und Nutzung dieser Daten richtet sich dabei nach den Leistungen und dem Funktionsumfang des Produktes.

Folgende Datenkategorien können vom Verantwortlichen durch direkte Eingabe oder durch Hochladen in allen Versionen der Softwareprodukte verarbeitet werden:

- *Angaben zu Nutzern:* Stammdaten Name, Vorname, Nutzername, E-Mail-Adresse
- *Angabe zu Nutzungszeitpunkt im Softwareprodult:* Zeitstempel und Nutzername des letzten Logins, durchgeführte Aktionen (Audit Log)

Alle Kernfunktionen der Softwareprodukte werden ausschließlich in Deutschland entwickelt und in Deutschland bzw. der EU (je nach Verfügbarkeit virtueller Server-Ressourcen des Infrastruktur-Partners Hetzner) gehostet. Darüber hinaus gibt es ergänzende Zusatzfunktionen (z.B. Supportplattform), bei der auf durch den Verantwortlichen genehmigte Subunternehmen (siehe **Anlage 1**) zurückgegriffen wird, die teilweise ihren Sitz außerhalb der EU/EWR haben.

Jede weitere Verlagerung einer Datenverarbeitung in ein Drittland außerhalb der EU/EWR darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Sofern und soweit ein Angemessenheitsbeschluss i.S.v. Art. 45 DSGVO vorliegt und für den jeweiligen Datenexport eingreift, stützen wir diesen in der Regel darauf. Sollte ein solcher nicht vorliegen, wurde mit dem jeweiligen Empfänger ein Vertrag mit Standarddatenschutzklauseln der Europäischen Kommission (Art. 46 Abs. 2 Buchstaben c und d DSGVO) geschlossen. Der Auftragsverarbeiter informiert den Auftraggeber rechtzeitig vor einer beabsichtigten Verlagerung des Ortes der Datenverarbeitung in ein Drittland. Der Auftraggeber kann der Änderung aus wichtigem Grund widersprechen.

2.2 Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfasst Mitbenutzer (User), die durch den Verantwortlichen zur Mitarbeit im jeweiligen Softwareprodukt freigeschaltet werden, z.B. Zuständige in der Gemeinde oder einer Behörde, oder eine Fachkraft im Kontext der Umsetzung des Gewässermanagements im Unternehmen oder der Behörde, oder Gemeinde des Verantwortlichen.

3. Technische und organisatorische Maßnahmen

3.1 Der Auftragsverarbeiter verpflichtet externe Rechenzentren sowie sonstige Unterauftragsverarbeiter, die innerbetriebliche Organisation so zu gestalten, dass es den besonderen Anforderungen des Datenschutzes gerecht wird. Insbesondere findet die Datenverarbeitung auf Datenverarbeitungsanlagen statt, für die das Rechenzentrum oder der sonstige Unterauftragsverarbeiter alle technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat.

3.2 Der Auftragsverarbeiter hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen (Einzelheiten in **Anlage 2**).

3.3 Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

4.1 Der Auftragsverarbeiter darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Verantwortlichen berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten.

4.2 Der Auftragsverarbeiter wird die Daten des Verantwortlichen nach dem Ende des Lizenzvertrages wie folgt behandeln:

1. Der Account bleibt für 1 Jahr in einem kostenlosem Read-Only Modus, mit dem Zweck die enthaltenen Daten ausleiten zu können.
2. Der Verantwortliche kann jederzeit vollständige Löschung verlangen.
3. Entschließt sich ein Verantwortlicher nach der kostenlosen Testphase nicht zum Kauf eines Abonnements, so wird der Testaccount nach einem letztmaligen Hinweis per E-Mail automatisch spätestens 1 Monat nach Beendigung der Testregistrierung gelöscht.

Darüber hinaus sind zusätzliche Löschkonzepte, das Recht auf Vergessenwerden, die Berichtigung und Auskunft vom Verantwortlichen sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

1. Der Ansprechpartner des Auftragsverarbeiters zum Thema Datenschutz ist: Dr. Andreas Stowasser, Telefon: 0351-32061500, E-Mail: datenschutz@stowasserservice.de
2. Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragsverarbeiter setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit (inklusive § 203 StGB) verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragsverarbeiter und jede dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Verantwortlichen verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

3. Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO (Einzelheiten in **Anlage 2**).

4. Der Verantwortliche und der Auftragsverarbeiter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

5. Die unverzügliche Information des Verantwortlichen über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragsverarbeiter ermittelt.

6. Soweit der Verantwortliche seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragsverarbeiter ausgesetzt ist, hat ihn der Auftragsverarbeiter nach besten Kräften zu unterstützen.

7. Der Auftragsverarbeiter kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen

Person gewährleistet wird.

8. Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Verantwortlichen im Rahmen seiner Kontrollbefugnisse nach Ziffer 8 dieses Vertrages.

6. Unterauftragsverhältnisse

6.1 Als Unterauftragsverhältnisse im Sinne dieses Vertrags sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragsverarbeiter z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice erbringt. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Verantwortlichen auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

6.2 Die Auslagerung auf Unterauftragsverarbeiter oder der Wechsel der bestehenden genehmigten Unterauftragsverarbeiter sind zulässig, soweit der Auftragsverarbeiter eine solchen Einschaltung von Unterauftragsverarbeitern dem Verantwortliche eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und der Verantwortliche nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragsverarbeiter schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird. Im Falle des Einspruchs des Verantwortlichen steht dem Auftragsverarbeiter ein außerordentliches Kündigungsrecht sowohl hinsichtlich dieser Vereinbarung als auch bezüglich der Leistungsvereinbarung zu.

6.3 Der Verantwortliche stimmt der Beauftragung der in der **Anlage 1** vor Beginn der Verarbeitung mitgeteilten Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zu.

6.4 Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragsverarbeiter die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.

6.5 Die Weitergabe von personenbezogenen Daten des Verantwortlichen an den Unterauftragsverarbeiter und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

7. Drittanbieter

Wir bieten Kooperationen mit externen Partnern an. Falls der Auftraggeber sich entschließt mit diesen Partnern direkte Verträge einzugehen, so ist er für den Abschluss

eines Vertrages zur Auftragsverarbeitung selbst zuständig.

8. Kontrollrechte des Verantwortlichen

8.1 Der Verantwortliche hat nach Vorankündigung das Recht, die Einhaltung der datenschutzrechtlichen Prozesse und der vertraglichen Vereinbarung durch den Auftragsverarbeiter oder das externe Rechenzentrum/den Unterauftragsverarbeiter zu kontrollieren. Dies kann entweder durch die Einholung von Auskünften oder die Vorlage von aktuellen Testaten, Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Revision, Datenschutzbeauftragter) oder durch eine geeignete Zertifizierung mittels IT-Sicherheits- oder Datenschutzaudit erfolgen. Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen.

8.2 Der Auftragsverarbeiter stellt sicher, dass sich der Verantwortliche von der Einhaltung der Pflichten des Auftragsverarbeiters nach Art. 28 DSGVO überzeugen kann. Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

9. Mitteilung bei Verstößen des Auftragsverarbeiters

9.1 Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

- die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
- die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Verantwortlichen zu melden
- die Verpflichtung, den Verantwortlichen im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
- die Unterstützung des Verantwortlichen für dessen Datenschutz-Folgenabschätzung
- die Unterstützung des Verantwortlichen im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

9.2 Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragsverarbeiters zurückzuführen sind, kann der Auftragsverarbeiter eine Vergütung beanspruchen.

10. Weisungsbefugnis des Verantwortlichen

10.1 Mündliche Weisungen bestätigt der Verantwortliche unverzüglich (mind. Textform).

10.2 Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird.

11. Löschung von personenbezogenen Daten

11.1 Kopien oder Duplikate der Daten werden ohne Wissen des Verantwortlichen nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

11.2 Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Verantwortlichen – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Testdaten. Das Protokoll der Löschung ist auf Anforderung vorzulegen. Für die Löschung der Daten in der Applikation gilt Nr. 4.

11.3 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben.

12. Schlussbestimmungen

Diese Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO tritt mit Beginn des Lizenzvertrages in Kraft.

Anlage 1: Unterauftragsverarbeiter

Der Verantwortliche stimmt der Beauftragung der nachfolgenden Unterauftragsverarbeiter zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO:

Unterauftragsverarbeiter

Nr	Firma	Anschrift	Leistung
1	StowasserPlan GmbH & Co. KG	Hauptstraße 47f, 01445 Radebeul	Fachliche Beratung
2	DrySoc GmbH	Kettenburg 5a, 27374 Visselhövede	Entwicklung & Support
3	MKDC Software UG (haftungsbeschränkt)	Katschhof 3, 52062, Aachen	Entwicklung & Support
4	Hetzner Online GmbH	Am Datacenter-Park 1, 08223 Falkenstein/Vogtland	Infrastruktur für den Betrieb von PROGEMIS
5	Microsoft Azure "Deutschland West Central"	Frankfurt am Main	Infrastruktur für den Betrieb von PROGEMIS
6	Microsoft Azure "West Europe"	Schiphol, Noord-Holland	Infrastruktur für den Betrieb von SOFIE
7	Amazon Web Services	Eschborner Landstraße 100, 60489 Frankfurt am Main	Speicherkapazität für die redundante Ablage von Backups

Nr	Firma	Anschrift	Leistung
8	Zoho Corporation GmbH	II. Hagen 7, 45127 Essen	Ticketsystem
9	Hubspot	Am Postbahnhof 17, 10243 Berlin	Kundenmanagement-System

Anlage 2: Technische und organisatorische Maßnahmen

der StowasserService GmbH & Co. KG

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1.1 Zutrittskontrolle:

- Gebäude allgemein:
  – Der Haupteingang des Gebäudes sowie der Zugang über die Tiefgarage sind durch Schlösser gesichert, die nur unter Benutzung von Sicherheitsschlüsseln zu öffnen sind. Die Büroeingangs-Tür ist nach Widerstandsklasse (WK) 3 Standard gesichert.
  – Besucher müssen sich bei ihrer Ankunft an- und bei ihrer Abreise abmelden. Während ihres Aufenthalts werden sie von Mitarbeiter:innen begleitet.
- Rechenzentrumsräume:
  – PROGEMIS Kundendaten werden in Rechenzentren von Azure (Rechenzentrum), "Deutschland West Central" verarbeitet und gespeichert
  - SOFIE Kundendaten werden in Rechenzentren von Azure (Rechenzentrum), "West Europe" verarbeitet und gespeichert
  - UferExpert Kundendaten werden in Rechenzentren von Azure (Rechenzentrum), "West Europe" verarbeitet und gespeichert

1.2 Zugangskontrolle:

- Der Benutzer- und Administratorzugriff auf das jeweilige System beruht auf einem rollenbasierten Zugriffsberechtigungsmodell. Jeder Nutzer erhält eine eindeutige ID, um sicherzustellen, dass alle Systemkomponenten nur von berechtigten Benutzern und Administratoren genutzt werden können.

- Es existieren technische Policies zur Passwortkomplexität
- Es gilt das Prinzip der Minimalberechtigung. Jeder Benutzer erhält nur die Zugriffsrechte, die erforderlich sind, um seine vertraglichen Tätigkeiten durchzuführen. Benutzerkonten werden immer zunächst mit den wenigsten Zugriffsrechten ausgestattet. Für die Einräumung von Zugriffsrechten über die Minimalberechtigung hinaus, muss eine entsprechende Berechtigung vorliegen
- Für alle Infrastruktur-Elemente ist Zwei-Faktor-Authentifizierung etabliert
- Einsatz von Firewallsystemen mit Intrusion Detection Systemen (IDS) und Intrusion Prevention Systemen (IPS), Virenscanner für sämtliche Serversysteme der in Abschnitt 1.1. genannten Produkte. Der Betrieb der Schutzmaßnahmen erfolgt durch Azure Deutschland
- Der Zugriff auf Serversysteme erfolgt SSH-verschlüsselt

1.3 Zugriffskontrolle:

- Zugriffsberechtigung auf Produktivsysteme ist auf einen kleinen Kreis von Mitarbeiter:innen (“Systemadministrator:innen”) beschränkt.
- Alle Zugriffe auf Produktivsysteme durch Systemadministratoren werden mit User-ID, Zeitstempel und Anlass protokolliert.

1.4 Trennungskontrolle:

- Datensätze unterschiedlicher StowasserService Kunden im selben Einzugsgebiet (z.B. Wasserwirtschaftsamt oder Gewässerunterhaltungsverband) werden in einer einheitlichen Datenbank speziell markiert (softwareseitige Mandantenfähigkeit).
- Datensätze unterschiedlicher StowasserService Kunden in unterschiedlichen Einzugsgebieten (z.B. Wasserwirtschaftsamt oder Gewässerunterhaltungsverband) werden in voneinander getrennten Datenbanken gespeichert (infrastrukturelle Mandantenfähigkeit).
- Test- und Produktivdaten sind strikt getrennt in unabhängigen Systemen, Entwicklungssysteme sind ebenfalls unabhängig von Test- und Produktivsystemen.
- Unterschiedliche Domains und SSL-Zertifikate für Test- und Produktivsysteme.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Datenübertragung zwischen Serversystemen erfolgt ausschließlich verschlüsselt. Soweit Daten zu beauftragten Partnern übertragen werden, sind diese Datenübertragungskanäle immer TSL verschlüsselt. Wo dies technisch möglich ist, kommen VPN-Verbindungen zum Einsatz. Änderungen an Datensätzen werden kontinuierlich protokolliert.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Es werden regelmäßig automatische Sicherungskopien und Backups aller Kundendaten erstellt. Es gibt ein dediziertes Konzept zur Rekonstruktion der Datenbestände und zudem eine regelmäßige Überprüfung, dass die Datensicherungen auch tatsächlich wieder eingespielt werden können (Datenintegrität der Backups). Es existiert ein Notfallkonzept

mit namentlich benannten Verantwortlichen und einer expliziten Vertreterregelung. Das Notfallkonzept wird regelmäßig überprüft und aktualisiert. Mitarbeiter:innen werden entsprechende des Notfallkonzepts in regelmäßigen Abständen auf dieses Notfallkonzept geschult. Backups und Sicherungskopien sind über mehrere redundante Serversysteme und Rechenzentrumsstandorte verteilt. Produktivsysteme sind mehrfach redundant ausgelegt. Backups werden regelmäßig auf Wiedereinspielbarkeit geprüft. Es gibt regelmäßige Notfallübungen, in denen Teams u.a. Wiederherstellungsszenarien üben.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

Für sämtliche Unternehmen in denen personenbezogenen Daten verarbeitet werden, wurde ein Datenschutzbeauftragter bestellt. Die StowasserService GmbH & Co. KG hat die Grundsätze des Datenschutzes in einer Datenschutzrichtlinie festgelegt.

Stand: 17.12.2025