Auftragsverarbeitungs-Vertrag gemäß Art. 28 Datenschutz-Grundverordnung (DS-GVO)

zwischen der

- nachstehend Auftraggeber genannt -

und der

billwerk GmbH
Mainzer Landstraße 51
60329 Frankfurt/
Main

- nachstehend Auftragnehmer genannt

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Der Gegenstand des Auftrags ergibt sich aus der Leistungsvereinbarung, dem „SaaS-Vertrag“ vom 16.10.2020, auf die hier verwiesen wird (im Folgenden Leistungsvereinbarung genannt).

Der Auftragnehmer bietet seinen Kunden verschiedene Dienstleistungen rund um die Abrechnung von Leistungen, insbesondere von Abo-Services, an. Diese erbringt der Auftragnehmer auf Basis der mit dem Auftraggeber vereinbarten Nutzungsbedingungen und Leistungsbeschreibungen. Diese Vereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus den einzelnen vom Auftraggeber beim Auftragnehmer gebuchten Leistungen (nachfolgend zusammengefasst „Hauptvertrag“ genannt) ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

(2) Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten
Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung vom 16.10.2020.

Der Auftragnehmer kann die vom Auftraggeber auf Test- und Sandboxsystemen erstellten und gespeicherten Testdaten in anonymisierter Form ausschließlich zu internen Testzwecken verwenden.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet bis auf die unter 7. genannten Fälle in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DS-GVO erfüllt sind.

(2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

Angaben zur Person:

- Stammdaten wie Name und Anschrift
- E-Mail-Adresse
- Telefonnummer
- Mobilfunknummer
- Bankverbindung
- Bestelldaten
- Rechnungsdaten
- Daten zum Zahlungsverhalten

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Kunden des Auftraggebers
- Ansprechpartner des Auftraggebers
- Zahlungsdienstleister des Auftraggebers

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Artt. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO 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 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 1].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer 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

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich oder mit der Bitte um Auskunft unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer die betroffene Person unverzüglich an den Auftraggeber verweisen.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

(1) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 38 und 39 DS-GVO ausübt.

Als Datenschutzbeauftragte(r) ist beim Auftragnehmer

Herr/Frau Vorname, Nachname: Ronald Baranowski

Organisationseinheit: extern

Telefon: 06101-982 94 22

E-Mail: rb@six-datenschutz.de

bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

(2) Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO.
Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen

Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers 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 Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].

(4) Auftraggeber und Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

(5) Die unverzügliche Information des Auftraggebers 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 Auftragnehmer ermittelt.

(6) Soweit der Auftraggeber 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 Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

(7) Der Auftragnehmer 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.

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

6. Mitwirkungspflichten des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12-23 DSGVO. Es gelten die Regelungen von Ziff. 11 dieses Vertrages.
(2) Der Auftragnehmer wirkt an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten durch den Auftraggeber mit. Er hat dem Auftraggeber die insoweit jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

7. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

Die Auslagerung auf Unterauftragnehmer ist zulässig, soweit:

a) der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und

b) eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO und, im Fall von Auslagerungen in Drittstaaten, wenn die besonderen Voraussetzungen der Art. 44 ff. EU-DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln), zu:

Firma Unterauftragnehmer	**Anschrift/Land**	**Leistung**
Gridscale GmbH	Oskar-Jäger-Str. 173 50825 Köln, Deutschland	Hosting billwerk Infrastruktur (Failover System)
Mailjet SAS	13-13 bis, rue de l'Aubrac – 75012 Paris, Frankreich	Mailversand
letterei.de Postdienste GmbH (Onlinebrief24)	Frankfurter Str. 74 64521 Groß-Gerau, Deutschland	Briefversand
Zendesk	1019 Market St San Francisco, CA 94103 USA	Helpdesk-SaaS
Amazon Web Services EMEA SARL	38 avenue John F. Kennedy, L-1855 Luxembourg	Hosting billwerk Infrastruktur / Failover-System. Ausschließlich auf Servern in der Region Europa/Frankfurt
OOO Billwerk / OOO Биллверк	Sovetskaya str 12, 3rd floor, 220030, Minsk, Weissrusland	Support-, Entwicklungs-, und Marketing-Ressourcen.

(2) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(3) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(4) Soweit während der Geltung dieses Vertrages ein Unterauftragnehmer/Wechsel vom Auftragnehmer beabsichtigt wird, informiert der Auftragnehmer den Auftraggeber mit einer Vorlaufzeit von 3 Kalendermonaten hierüber. Die Zustimmung des Auftraggebers hierüber gilt als erteilt, sofern er nicht innerhalb von 20 Werktagen nach Zugang der Information einen Widerspruch erklärt. Der Widerspruch darf nicht willkürlich und nur aus wichtigen datenschutzrechtlichen Gründen erfolgen. Sollte der Auftraggeber mit der Wahl des neuen Unterauftragnehmers nicht einverstanden sein und eine Einigung nicht möglich ist, stehen Auftraggeber und Auftragnehmer ein Sonderkündigungsrecht zu.

8. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen. Der Auftraggeber verpflichtet sich, die durch eine Kontrolle verursachten angefallenen Kosten zu tragen. Die Höhe der angefallenen Kosten hat der Auftragnehmer nachzuweisen. Für die Berechnung wird ein Stundensatz von 100 Euro pro Mitarbeiter zugrunde gelegt, zuzüglich eventuell anfallender Mehrwertsteuer und Fremdkosten (z.B. externer DSB).

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

a) die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;

b) die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;

c) aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);

d) eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

9. Mitteilung bei Verstößen des Auftragnehmers

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

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

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden

c) die Verpflichtung, den Auftraggeber bei der Erfüllung seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12-23 DSGVO zu unterstützen und ihm in diesem Zusammenhang sämtliche Informationen unverzüglich zur Verfügung zu stellen

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

10. Weisungsbefugnis des Auftraggebers

(1) Der Auftraggeber hat jederzeit das Recht, Weisungen zu Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen des Auftraggebers erfolgen in der Regel schriftlich.

(2) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(3) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

11. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers 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.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

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

12. Schlussbestimmungen

(1) Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.

(2) Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

(3) Für Nebenabreden ist die Schriftform erforderlich.

(4) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

(5) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

(6) Es gilt deutsches Recht.

Auftraggeber:

_____

Ort, Datum rechtsverbindliche Unterschrift

Auftragnehmer:

_____

Ort, Datum rechtsverbindliche Unterschrift

Anlage 1

Technisch/-organisatorische Maßnahmen nach Art. 32 DS-GVO bzw. §64 BDSG (neu)

Unternehmen: billwerk GmbH

Firmensitz: Mainzer Landstr. 51, 60329 Frankfurt

Unternehmensführung: Dr. Ricco Deutscher – CEO –

IT-Abteilung: Jonas Hornung, CIO, jonas.hornung@billwerk.com, T. +49 69 348779926

Datenschutzbeauftragter: Ronald Baranowski, SIX DATENSCHUTZ, Frankfurter Str. 146, 61118 Bad Vilbel

Prüfdaten:

Prüfung am:

Prüfung durch:

Geprüfte Orte:

Auditinterviews:

Am:_____mit:_____Unterschrift:_____

Am:_____mit:_____Unterschrift:_____

Erläuterung: Die billwerk Applikation wird gehostet auf Servern der Gridscale GmbH (GS) und der Amazon Web Services Inc. (AWS).

1 Zutrittskontrolle

Alle Angaben zu den Rechenzentren von Amazon Web Services können hier: https://aws.amazon.com/de/compliance/data-center/data-centers/ überprüft werden.

Die Nachweise in diesem Kapitel, die sich auf das Rechenzentrum bei AWS beziehen, stammen von der Website https://aws.amazon.com/de/compliance/data-center/controls/

1.1 Technische Maßnahmen:

	Maßnahme	Bemerkung/Nachweis:
☒	Alarmanlage/Einbruchmeldeanlage	„In der Datenebene sind elektronische Einbruchmeldesysteme installiert, die sicherheitsrelevante Ereignisse erkennen und automatisch die zuständigen Mitarbeiter alarmieren. Die Ein- und Ausgänge der Serverräume sind durch Geräte gesichert, an denen Personal Multi-Faktor-Authentifizierungsverfahren durchlaufen müssen, bevor sie den Raum betreten oder verlassen können. Diese Geräte lösen einen Alarm aus, wenn die Tür ohne Autorisierung aufgebrochen oder offengehalten wird. Die Türalarmsysteme sind so konfiguriert, dass sie erkennen, wenn jemand eine Datenebene ohne Multi-Faktor-Autorisierung betritt oder verlässt. In diesem Fall wird umgehend ein Alarm ausgelöst und an die AWS Security Operations Center zur Protokollierung, Analyse und Reaktion gesendet.“
☒	automatisiertes Zutrittskontrollsystem (z.B. Kartenleser, Zahlencode, Transponder-Schließsystem)	„Der physische Zugang wird durch professionelles Sicherheitspersonal an den Gebäudeeingängen kontrolliert. Dabei werden Überwachung, Meldeanlagen und andere elektronische Vorrichtungen eingesetzt. Autorisiertes Personal erlangt über Multi-Faktor-Authentifizierungsmechanismen Zugang zu den Rechenzentren. Die Eingänge zu den Serverräumen sind mit Geräten abgesichert, die Alarm auslösen, wenn die Tür aufgebrochen oder offen gehalten wird.“
☒	Kameraüberwachung Videoüberwachung der Zugänge zum Unternehmen	„Physische Zugangspunkte zu Serverräumen werden von CCTV-Kameras mit Aufzeichnungsfunktion überwacht. Die Aufnahmen werden gemäß behördlichen und Compliance-Anforderungen aufbewahrt.“
☒	Manuelles Schließsystem (Sicherheitsschloss)	Personalschränke sind immer verschlossen. Schlüssel bei CEO Dr. Ricco Deutscher Bürofläche der billwerk GmbH wird nach Arbeitsende verschlossen.

☒	Sicherheitsverfahren für Home-office u. bei Reisen	Homeoffice-Richtlinie vorhanden, Zugriff auf die Server nur via VPN
☒	Sonstige	Die Serverräume von AWS werden von einem Sicherheitspersonal überwacht

1.2 Zugangskontrolle

1.2.1 Technische Maßnahmen:

	Maßnahme	**Bemerkung/Nachweis:**
☒	Benutzer-/Passwortverfahren mit wenigstens 8 Zeichen, drei Zeichenklassen und erzwungenem Passwortwechsel nach spätestens drei Monaten	Passwortmindestlänge ist 8; bei gleichzeitiger Festlegung auf alphanumerische Zeichen und Sonderzeichen. Automatische Bildschirmsperren auf den Arbeitsstationen/Notebooks; Siehe Password-Policy
☒	Public Key Infrastructure (PKI)	Zugang zu den Linux-Servern wird mit dem Public-Key-Verfahren geregelt
☒	Einsatz von Anti-Viren-Software	Auf allen Windows-Systemen ist Microsoft Essentials installiert
☒	Einsatz von Firewalls	In der IT-Umgebung des Unternehmens werden verschiedene Firewalls und Systeme für die IT-Sicherheit eingesetzt.
☒	Logging aller Zugriffsversuche	Standard-Logging auf allen Servern aktiv
☒	Einsatz von VPN Technologie	Mitarbeiter im Homeoffice, die auf Server zugreifen möchten, verbinden sich via VPN mit dem billwerk-office-Netzwerk um eine in der Firewall freigeschaltete IP zu erhalten
☒	Verschlüsselung	Verschlüsselung des Datenbank-Storages auf Betriebssystemebene, zusätzlich zur Verschlüsselung auf Serverebene durch AWS

	Maßnahme	Bemerkung/Nachweis:
☒	Verschlüsselung von Datenträgern	Festplatten der billwerk-Notebooks sind verschlüsselt, externe Festplatte für Laptop-Backups ist verschlüsselt; Storage-Server sind verschlüsselt
☒	Getrennte Benutzerkonten für Systemadministration und User	Serverzugriff nur für Administratoren, bei Linux-Servern: root-Zugriff nur mit zusätzlichem Sudo-Passwort
☒	Die Tätigkeiten der Systemadministration an den IT-Systemen werden protokolliert …	Protokolle werden in zentralem Wiki-System gespeichert
☒	… diese Protokolldateien werden regelmäßig ausgewertet	Monatliche Prüfung der Protokolldateien
☒	Einsatz eines Intrusion Detection Systems	Netzwerkübergreifendes Intrusion Detection System (AWS Guardduty).

Wie erfolgt der Zugang ins Internet?

	Maßnahme	Bemerkung/Nachweis:
☒	Über eine Sicherheitsinfrastrukturkette aus, Virenscanner und Firewall für Server, Endgeräte, neue Geräte	Alle Client-Rechner verfügen über einen Virenscanner und eine eigene Firewall

1.2.2 Organisatorische Maßnahmen:

	Maßnahme	Bemerkung/Nachweis:
☒	Benutzerberechtigungen werden vergeben und verwaltet	Gruppenberechtigungen, Verzeichnisrechte, Berechtigungen für Anwendungen, Serverzugriffsrechte, werden durch Systemadminstrator verwaltet und zugewiesen
☒	Benutzerprofile werden erstellt	
☒	Sorgfältige Auswahl des Reinigungspersonals und anderer Dienstleister im Unternehmen	
☒	Sorgfältige Auswahl des Sicherheitspersonals	Die Hosting-Dienstleister beschäftigen Sicherheitspersonal, das sie selbst auswählen
☒	Clean-Desk-Policy	Mitarbeiter der billwerk GmbH müssen vertrauliche Dokumente/Daten/Datenträger vor Verlassen des Arbeitsplatzes sicher verwahren (abschließbare Schränke)

1.3 Zugriffskontrolle

1.3.1 Technische Maßnahmen

	Maßnahme	**Bemerkung/Nachweis:**
☒	Einsatz von Aktenvernichtern	Aktenvernichter vorhanden
☒	Ordnungsgemäße Vernichtung von Datenträgern (gem. DIN 32757)	Vernichtung von digitalen Datenträgern bisher nicht nötig gewesen
☒	Physische Löschung von Datenträgern vor deren Wiederverwendung	Sollten Datenträger wiederverwendet werden, werden sie vorher sorgfältig gelöscht
☒	Protokollierung der Vernichtung von Daten	
☒	Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten	-
☒	Verschlüsselung von Datenträgern	- Windows-Laptops der billwerk GmbH mit Bitlocker oder VeraCrypt verschlüsselt (je nach Windows-Version) - Macbooks der billwerk GmbH mit FileVault verschlüsselt - Externe Festplatte für Backups mit Bitlocker verschlüsselt
☒	Anwendung eines differenzierten, schriftlichen Berechtigungskonzepts, um die Nutzung von Profilen bzw. Rollen und Transaktionen zu regeln → für Anwendungen wie z.B. OneDrive → für Filesystem werden Berechtigungen vom Owner freigegeben	Zugriff auf vertrauliche Dokumente wird über das Berechtigungssystem des Dokumentenmanagementsystems OneDrive geregelt. Zugriff auf Endkundendaten nur für Systemadministratoren und Kundenbetreuer/Support-Mitarbeiter. Zugriff auf Serversysteme nur für Systemadministratoren und Mitglieder des Notfall-Teams. Zugriff auf Personaldaten hat nur die Personalabteilung
☒	Maßnahmen zur Vermeidung unberechtigten Eindringens (Intrusion detection and prevention)	Die Serversysteme werden mit Firewalls gegen unberechtigtes Eindringen gesichert. Zusätzlich ist auf allen Servern ein Intrusion Detection System installiert.
☒	Regelmäßige Installation Software- und Betriebssystem-Updates	Die Software der Serversysteme wird einmal pro Monat aktualisiert. Dabei werden die Updates zunächst auf Testsystemen installiert, bevor sie auf den Produktivsystemen ausgerollt werden
☒	Zeitnahe Installation von Sicherheitskritischen Updates	Sollte kritische Sicherheitslücken erkannt und vom jeweiligen Softwarehersteller durch Updates behoben werden, werden diese Updates schnellstmöglich installiert. Um die Funktionalität der Software sicherzustellen, werden die Updates zunächst auf Testsystemen, dann auf den Produktivsystemen installiert

Sichere Entwicklung

☒	Vermeidung typischer Angriffsmuster durch Standardvorgehen und –Bibliotheken	Wird durch die Entwicklungsleitung vorgegeben und durch Codereviews kontrolliert
☒	Code Repositories	Billwerk hat eigenen GitHub-Account. Der Zugriff auf den Account und die Repositories werden durch die Entwicklungsleitung und die Systemadministratoren verwaltet
☒	Code Reviews	Durch Code-Reviews wird überprüft, ob die Entwicklungsrichtlinien eingehalten wurden, bzw. es wird sichergestellt, dass keine Sicherheitslücken eingebaut werden. Verantwortlich für die Code-Reviews ist die Entwicklungsleitung
☒	Unit Tests	Unit Tests stellen sicher, dass sich das Standardverhalten von bekannten Geschäftsfällen nicht ändert. Auch hierdurch können gegebenenfalls Sicherheitsproblematiken erkannt werden.
☒	QA / Testing	Das QA Team untersucht einen Release Candidate funktional nach möglichen Sicherheitsproblematiken. Auf einem Testsystem kann ein Release Candidate automatisiert gezielt auf Schwachstellen für diverse Angriffsszenarien getestet werden

1.3.2 Organisatorische Maßnahmen

	Maßnahme	**Bemerkung/Nachweis:**
☒	Die Anzahl der Systemadministratoren ist auf das Notwendigste reduziert	Nur die Systemadministratoren und die Mitglieder des Bereitschaftsteams haben Administrator-Zugriff auf die Server-Systeme
☒	Es existiert ein Berechtigungskonzept mit geringst-möglichen Zugriffsrechten (only rights required to do the job)	Teil der Security-Policy
☒	Passwortrichtline inkl. Länge und Wechsel (s.o.)	Password-Policy vorhanden
☒	Sichere Aufbewahrung von Datenträgern	Datenträger werden nach Feierabend verschlossen aufbewahrt, digitale Datenträger, die sensible Daten enthalten (z.B. externe Festplatte für Backups) sind verschlüsselt
☒	Verwaltung der Benutzerrechte durch Systemadministratoren	
☒	Es existieren schriftliche Regelungen zur Nutzung mobiler Datenträger (CD, DVD, USB-Stick, etc.)	Teil der Security-Policy
☒	Verwaltung der Benutzeraccounts-durch Systemadministratoren	Sollte ein Mitarbeiter aus dem Unternehmen ausscheiden, werden alle Accounts und Berechtigungen des Mitarbeiters unverzüglich gelöscht

Protokollierung von Systemzugriffen durch Benutzer

☒	Alle Systemzugriffe werden protokolliert	Auf Serversystemen läuft das Standard-Logging, das alle Zugriffe protokoliert
☒	Sonstiges (bitte nachfolgend erläutern)	Administrative Aktivitäten werden manuell protokolliert

Die Protokolle werden wie folgt ausgewertet:

☒	Bei Bedarf	

1.4 Trennungskontrolle

1.4.1 Technische Maßnahmen

	Maßnahme	Bemerkung/Nachweis:
☒	Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern	
☒	Trennung von Produktiv- und Testsystem	
☒	Bei Inanspruchnahme von Cloud-Services: single tenant setup für Applikationen und Daten	

1.4.2 Organisatorische Maßnahmen

	Maßnahme	Bemerkung/Nachweis:
☒	Ein Berechtigungskonzept liegt vor	Serverzugriffe nur für Systemadministratoren oder Mitglieder des Bereitschaftsteams, Root-Rechte nur mit zusätzlichem Kennwort verfügbar; Siehe Security-Policy
☒	Datenbankrechte sind definiert	Datenbankzugriff nur für Systemadministratoren oder Mitglieder des Bereitschaftsteams
☒	Eine logische Mandantentrennung wird durchgeführt	
☒	Es existieren schriftliche Regelungen zur Funktionstrennung (z.B. Test/Produktion, Mandantentrennung)	Getrennte Hardware für Produktiv- und Testsysteme; Mandanten werden von der Applikation als „Entities“ getrennt behandelt

Wie wird sichergestellt, dass Daten nur zum vorgesehenen Zweck verarbeitet und genutzt werden?

☒	Es gibt eine Trennung zwischen Entwicklung, Test und Produktion	
☒	Datentrennung durch ein differenziertes Benutzerkonzept	
☒	Die Daten werden nach Mandanten getrennt verarbeitet	

1.5 Pseudonymisierung/Anonymisierung

1.5.1 Technische Maßnahmen

	Maßnahme	Bemerkung/Nachweis, Beschreibung des Verfahrens:
☒	folgende Daten werden pseudonymisiert/anonymisiert:	Pseudonymisierung bisher nicht möglich, da extrem hoher Aufwand und Kosten, zudem starke Verkomplizierung der Arbeit

2 Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

2.1 Weitergabekontrolle

2.1.1 Technische Maßnahmen

	Maßnahme	Bemerkung/Nachweis:
☒	Daten-Verschlüsselungen	Storages der Serversysteme sind verschlüsselt
☒	Verschlüsselung von Speichermedien mobiler Endgeräte (z.B. Laptops)	Festplatten der Windows-Notebooks sind mit Bitlocker oder VeraCrypt verschlüsselt, Festplatten Mac-Notebooks sind mit FileVault verschlüsselt

Wie werden die Daten beim (physikalischen) Transport geschützt?

	Maßnahme	Bemerkung/Nachweis:
☒	Nicht relevant, weil kein Transport von Daten(trägern) stattfindet.	

2.1.2 Organisatorische Maßnahmen

	Maßnahme	Bemerkung/Nachweis:
☒	Nicht relevant, weil kein Transport von Daten(trägern) stattfindet.	

2.2 Eingabekontrolle

2.2.1 Technische Maßnahmen

	Maßnahme	Bemerkung/Nachweis:
☒	Protokollierung der Eingabe, Änderung und Löschung von Daten mit Zeitstempel, User-IDs	Eingabe, Änderung und Löschung von Daten werden protokolliert

2.2.2 Organisatorische Maßnahmen

	Maßnahme	Bemerkung/Nachweis:
☒	Zufallszugriffe	

Wie werden diese Protokolle ausgewertet?

☒	Bei Bedarf	

3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

3.1 Verfügbarkeitskontrolle

3.1.1 Technische Maßnahmen

	Maßnahme	Bemerkung/Nachweis:
☒	Feuerlöschgeräte in Serverräumen	
☒	Feuer- und Rauchmeldeanlagen	
☒	Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen	
☒	Klimaanlage in Serverräumen	Klimaanlagen sind redundant ausgelegt
☒	Schutzsteckdosenleisten in Serverräumen	
☒	Unterbrechungsfreie Stromversorgung (USV) u/o Notstromgenerator	
☒	Gedoppelte Daten- und Telefonleitungen	
☒	Gedoppelte Energieleitungen	
☒	Daten Backups werden regelmäßig durchgeführt (täglich sowie weiter zeitlich geplante Backups)	Snapshot Backups werden regelmäßig von allen Datenbank Servern (alle 2 Stunden) gemacht und etwa einen Monat lang aufbewahrt
☒	Spiegelung von Daten und dem System	
☒	Getrennte Aufbewahrung von Produktivdaten und Datensicherungen	
☒	Stichprobenartige Prüfung von Datensicherungen (→ Backup fehlerfrei gelaufen)	täglich
☒	Einsatz von Virenscannern auf Arbeitsstationen	
☒	Einsatz von Virenscannern auf Servern	
☒	Einsatz von Firewalls zur Absicherung von Netzwerkübergängen	
☒	Einsatz von Personal Firewalls auf Arbeitsstationen	
☒	PEN (Penetrationstests) zur Überprüfung der Sicherheitsmechanismen, Risikoanalyse, Analyse und Beurteilung der Sicherheitsstandards	Werden von einem externen Dienstleister durchgeführt

3.1.2 Organisatorische Maßnahmen

	Maßnahme	**Bemerkung/Nachweis:**
☒	Alarmmeldung bei unberechtigten Zutritten zu Serverräumen	
☒	Aufbewahrung der Datensicherung an einem sicheren externen Ort	
☒	Erstellen eines Backup- und Disaster Recovery Konzepts	Halbtägliche Erstellung von sogenannten Snapshots, die auf andere Storages verschoben werden und schnell wiederhergestellt werden; Tägliche Erzeugung eines Datenbank-Dumps;
☒	Datenwiederherstellungen, regelmäßiges Testen von Disaster-Fällen	Datenwiederherstellung wird regelmäßig getestet
☒	Die Serverräume befinden sich nicht unterhalb sanitärer Anlagen	

3.2 Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

3.2.1 Technische Maßnahmen

	Maßnahme	**Bemerkung/Nachweis:**
☒	Ausfallrechenzentrum	Daten werden zu zweitem IaaS-Anbieter dupliziert (Cold Standby)
☒	gedoppelte Server, räumlich getrennt	Redundante Hardware in getrennten Netzwerkzonen (Fällt eine Zone aus, ist die zweite betriebsbereit)

3.2.2 Organisatorische Maßnahmen

	Maßnahme	**Bemerkung/Nachweis:**
☒	Notfallkonzept	

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

4.1 Datenschutz-Management

4.1.1 Technische Maßnahmen

	Maßnahme	Bemerkung/Nachweis:
☒	DMS existiert	

4.1.2 Organisatorische Maßnahmen

	Maßnahme	Bemerkung/Nachweis:
☒	Sensibilisierung der Mitarbeiter auf Datenschutz	Schulung hat stattgefunden, wird 1x jährlich wiederholt
☒	Informationssystem Fachabteilungen → DSB	Alle Datenschutz-Themen werden über den CIO an den DSB herangetragen…
☒	Informationssystem DSB → Fachabteilungen	…und vom CIO wieder an die Fachabteilungen zurückgegeben. Gibt es wichtige Hinweise vom DSB, werden alle Mitarbeiter benachrichtigt;
☒	Abarbeiten von Maßnahmen nach Projektmanagement-Systematik	Externe Anfragen zum Datenschutz (z.B. Lösch- oder Auskunftsanfragen) werden über das Support-Portal Zendesk an den Support gemeldet. Der Support benachrichtigt den CIO, der sich mit dem DSB zur Behandlung der Anfrage abstimmt;

4.2 Incident-Response-Management

4.2.1 Technische Maßnahmen

	Maßnahme	Bemerkung/Nachweis:
☒	es existiert in IRM-System	Incidents werden durch verschiedene Monitoring-Systeme gemeldet und durch das Team bearbeitet. Alle Incidents werden inklusive Workarounds oder Lösungen protokolliert, Sollten Änderungen notwendig werden, wird über das Projektmanagement ein Ticket eröffnet

4.2.2 Organisatorische Maßnahmen

	Maßnahme	Bemerkung/Nachweis:
☒	Notfall-Team bestehend aus: - Geschäftsleitung - IT-Leitung - Datenschutzbeauftragter	Notfall-Team kümmert sich um die Aufnahme von Incidents, gibt diese an die richtige Stelle weiter, bzw. kümmert sich eigenständig um eine Lösung.

4.3 Datenschutzfreundliche Voreinstellungen – Privacy by Default – (Art. 25 Abs. 2 DS-GVO)

4.3.1 Technische Maßnahmen

	Maßnahme	Bemerkung/Nachweis:

☒	Kunden, Interessenten	Anmeldung für Newsletter nur möglich, wenn Datenschutzbedingungen akzeptiert und Zustimmung zu Telefon- und E-Mail-Kontakt gegeben ist. Benutzerkonten für die billwerk-Plattform werden vom Kunden selbst angelegt; Rechteverwaltung wird vom Inhaber des Administrator-Kontos des jeweiligen billwerk-Kunden durchgeführt

4.3.2 Organisatorische Maßnahmen

	Maßnahme	**Bemerkung/Nachweis:**
☐	weitere	

4.4 Auftragskontrolle

4.4.1 Organisatorische Maßnahmen

	Maßnahme	**Bemerkung/Nachweis:**
☒	Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)	Es werden nur Hosting-Dienstleister ausgewählt, deren Hosting-Center in Deutschland sind und die ISO Norm 270001 erfüllen, sowie ausreichende Sicherheitsstandards erfüllen
☒	Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten	
☒	Schriftliche Weisungen an den Auftragnehmer gem. Art. 28 DSGVO i.V.m. Art. 29 DSGVO	Weisungen an die Hosting-Dienstleister werden per E-Mail, bzw. über Ticketing-System eingegeben
☒	Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags	
☒	Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis	
☒	Vorherige Prüfung der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen und entsprechende Dokumentation	TOMs der Hosting-Dienstleister liegen vor und wurden geprüft
☒	Wirksame Kontrollrechte gegenüber dem Auftragnehmer sind vereinbart	
☒	Der Auftragnehmer hat einen Datenschutzbeauftragten bestellt	