Vereinbarung zur Auftragsdatenverarbeitung

zwischen

- Auftraggeber -

und

billwerk GmbH, Mainzer Landstraße 33a, 60329 Frankfurt/Main

- Auftragnehmer -

Präambel

Der Auftragnehmer bietet seinen Kunden verschiedene Dienstleistungen rund um die Abrechnung von Leistungen, insbesondere von Abo-Services, an. Diese erbringt der Aufragnehmer 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. Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des Hauptvertrags.

1. Anwendungsbereich und Verantwortlichkeit

1.1 Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Hauptvertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich („verantwortliche Stelle“ im Sinne des § 3 Abs. 7 BDSG).

1.2 Die Weisungen werden durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die über die vertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

2. Betroffene, Datenarten und Verarbeitungszweck

2.1 Betroffene Personengruppen

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

2.2 Datenarten

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

2.3 Der Umfang der Datenverarbeitung ergibt sich aus dem Hauptvertrag.

2.4 Zweck der Datenverarbeitung ist allein die Bereitstellung der vom Auftragnehmer angebotenen Dienstleistungen für die Abrechnung der Leistungen des Auftraggebers gegenüber dem Kunden des Auftraggebers.

3. Pflichten des Auftragnehmers

3.1 Der Auftragnehmer darf Daten nur im Rahmen des Auftrages und der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen.

3.2 Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen des Bundesdatenschutzgesetzes (Anlage zu § 9 BDSG) entsprechen. Die vom Auftragnehmer getroffenen Maßnahmen sind in **Anlage 1** festgelegt. Eine Änderung der getroffenen Maßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

3.3 Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen per Verpflichtung untersagt ist, die Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis entsprechend § 5 BDSG). Das Datengeheimnis besteht auch nach Beendigung des Auftrages fort.

3.4 Der Auftragnehmer teilt dem Auftraggeber die Kontaktdaten des betrieblichen Datenschutzbeauftragten mit oder, falls keine Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten besteht, die Kontaktdaten des für die Datenverarbeitung verantwortlichen Mitarbeiters.

3.5 Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei schwerwiegenden Verstößen des Auftragnehmers oder der bei ihm im Rahmen des Auftrags beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder die im Vertrag getroffenen Festlegungen. Er trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab. Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung der Informationspflichten nach § 42a BDSG.

3.6 Etwa überlassene Datenträger sowie sämtliche hiervon gefertigten Kopien oder Reproduktionen verbleiben im Eigentum des Auftraggebers. Der Auftragnehmer hat diese sorgfältig zu verwahren, so dass sie Dritten nicht zugänglich sind. Der Auftragnehmer ist verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit seine Daten und Unterlagen betroffen sind. Die datenschutzkonforme Vernichtung von Test- und Ausschussmaterial übernimmt der Auftragnehmer auf Grund einer Einzelbeauftragung durch den Auftraggeber. In besonderen, vom Auftraggeber zu bestimmenden Fällen erfolgt eine Aufbewahrung bzw. Übergabe.

3.7 Der Auftragnehmer verwendet die überlassenen Daten für keine anderen Zwecke als die der Vertragserfüllung.

3.8 Die Erfüllung der vorgenannten Pflichten ist vom Auftragnehmer zu kontrollieren und in geeigneter Weise nachzuweisen.

4. Pflichten des Auftraggebers

4.1 Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

4.2 Die Pflicht zur Führung des öffentlichen Verfahrensverzeichnisses (Jedermannverzeichnis) gem. § 4g Abs. 2 S. 2 BDSG liegt beim Auftraggeber.

4.3 Der Auftraggeber legt die Maßnahmen zur Rückgabe der überlassenen Datenträger und/oder Löschung der gespeicherten Daten nach Beendigung des Auftrages vertraglich oder durch Weisung fest. Entstehen nach Vertragsbeendigung zusätzliche Kosten durch die Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

4.4 Erteilt der Auftraggeber Einzelweisungen, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, sind die dadurch begründeten Kosten vom Auftraggeber zu tragen.

5. Anfragen Betroffener an den Auftraggeber

Ist der Auftraggeber auf Grund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu geben, wird der Auftragnehmer den Auftraggeber dabei unterstützen, diese Informationen bereit zu stellen, vorausgesetzt der Auftraggeber hat den Auftragnehmer hierzu in Textform (§ 126b BGB) aufgefordert und der Auftraggeber erstattet dem Auftragnehmer die durch diese Unterstützung entstandenen Kosten.

6. Kontrollpflichten

6.1 Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers und dokumentiert das Ergebnis. Hierfür kann er Selbstauskünfte des Auftragnehmers einholen, sich vom Auftragnehmer eingeholte Sachverständigenberichte oder Prüfzertifikate vorlegen lassen oder auf eigene Kosten eine Prüfung durch einen zur Berufsverschwiegenheit verpflichteten Sachverständigen durchführen lassen. Eine solche Prüfung muss zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs erfolgen und bedarf einer angemessenen Vorankündigung.

6.2 Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung in Textform (§ 126b BGB) innerhalb einer angemessenen Frist alle Auskünfte zu geben, die zur Durchführung einer Prüfung erforderlich sind.

7. Unterauftragnehmer

7.1 Die Erteilung von Unteraufträgen durch den Auftragnehmer ist zulässig, sofern sich der Auftragnehmer vor Erteilung des jeweiligen Unterauftrages davon überzeugt, dass der Unterauftragnehmer geeignete und angemessene technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten getroffen hat.

7.2 Erteilt der Auftragnehmer Aufträge an Unterauftragnehmer, so obliegt es dem Auftragnehmer, seine Pflichten aus diesem Vertrag dem Unterauftragnehmer zu übertragen. Die Auftragserteilung muss schriftlich erfolgen. Satz 1 gilt insbesondere für Anforderungen an Vertraulichkeit, Da-

tenschutz und Datensicherheit zwischen den Vertragspartnern dieser Vereinbarung. Die regelmäßige Kontrolle der Unterauftragnehmer sowie die Dokumentation der Kontrollen obliegen dem Auftragnehmer. Der Auftragnehmer hat dem Auftraggeber auf Verlangen die Dokumentation seiner Kontrollen bereitzustellen.

7.3 Der Auftragnehmer hat den Auftraggeber auf Verlangen eine aktuelle Liste der eingesetzten Unterauftragnehmer zu übersenden.

8. Informationspflichten, Schriftformklausel, Rechtswahl

8.1 Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als „verantwortlicher Stelle“ im Sinne des Bundesdatenschutzgesetzes liegen.

8.2 Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragnehmers - bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

8.3 Es gilt deutsches Recht.

Anlage 1 Technische und organisatorische Maßnahmen des Auftragnehmers

Frankfurt, den

Auftraggeber	Auftragnehmer

Abschnitt I: Rechenzentrum

I.1. Zutrittskontrolle

- Der Zutritt zu den Räumlichkeiten ist für Dritte nur nach Klingeln und anschließender Anmeldung möglich.
- Besucher werden von einer Mitarbeiterin oder Mitarbeiter persönlich abgeholt und müssen sich dann anmelden. Sie erhalten anschließend einen Besucherausweis der offen zu tragen ist. Dieser ist beim Verlassen der Räumlichkeiten wieder abzugeben. Die Vergabe und Abgabe des Ausweises wird protokolliert.
- Der Zutritt zu den Rechenzentren, in denen sich sämtliche datenverarbeitenden Systeme und Speichersysteme befinden, ist physisch besonders gesichert.
- Das Rechenzentrum und die Zugänge zur Bürofläche werden videoüberwacht. Der Service Desk verfügt über Monitore für die Videokameras.
- Der Service Desk ist rund um die Uhr an 365 Tagen im Jahr besetzt.
- Der Notausgang des Rechenzentrums ist alarmgesichert.
- Zutritt zum Rechenzentrum wird nur autorisierten Personen gegeben. Autorisierte Personen sind in diesem Zusammenhang die zuständigen Mitarbeiter des Rechenzentrumsbetreibers sowie die zum Zeitpunkt des Vertragsabschlusses definierten Ansprechpartner von Kunden, diese aber nur in Bezug auf ihre eigenen Systeme. Der Zutritt zu anderen Systemen ist nicht erlaubt und wird überwacht
- Das Rechenzentrum verfügt für Mitarbeiter über ein elektronisches Zutrittssystem, separierte Bereiche des Rechenzentrums sowie die Büroräumlichkeiten. Die Zutrittsrechte werden auf den jeweiligen Zutrittskarten oder Tokens der Mitarbeiter gespeichert und sind zeitlich begrenzt. Der Prozess zur Zuteilung der Rechte zum Rechenzentrumszutritt auf dem jeweiligen Zutrittskarten oder Token ist dokumentiert.
- Lieferanten, Kunden und sonstigen Dienstleistern wird nur nach Anmeldung, Identifikation und Registrierung sowie in Begleitung der Zutritt zum Rechenzentrum gewährt.
- Alle Serversysteme befinden sich in abgeschlossenen Schränken (Racks). Nur die Mitarbeiter, die zum Zutritt ins Rechenzentrum berechtigt sind, haben auch Zugriff auf die Schlüssel zu den Schränken.
- Die Systeme, für die Dienstleistungen im Sinne der Auftragsdatenverarbeitung erbracht werden, befinden sich in einem separierten Abschnitt des Rechenzentrums. Kunden erhalten keinen Zutritt zu diesem Abschnitt.

I.2. Zugangskontrolle

- Der elektronische Zugang zu Systemen über Netzwerk ist durch Firewalls und VPNs geschützt.
- Die administrativen Zugangsdaten zu den jeweiligen Serversystemen sind nur den Administratoren bekannt.
- Jeder Nutzer erhält einen personalisierten, passwortgeschützten Account.
- Das Passwort ist im Abstand von 60 Tagen zu ändern und muss eine Kombination aus Buchstaben und Ziffern beinhalten. Dabei können die letzten 5 Passworte nicht wiederverwendet werden. Dies ist in der Sicherheitsrichtlinie Passwort-Policy dokumentiert. Wird ein Passwort nicht innerhalb der Frist geändert, wird der Account gesperrt.
- Zu Kundensystemen erhalten nur die Administratoren Zugriff, die den Kunden betreuen.
- Der Prozess zur Rechtevergabe ist dokumentiert.

I.3. Zugriffskontrolle

- Zu Kundensystemen erhalten nur die Administratoren Zugriff, die den Kunden betreuen.
- Zugriff auf Applikationen und Datenbanken wird – wo technisch realisierbar – rollenbasierend vergeben. Wo dies technisch nicht realisierbar ist, wird der Zugriff personenabhängig und individuell, je nach Aufgabenart, vergeben.

- Der Zugriff auf Netzlaufwerke erfolgt gemäß Benutzer(-gruppen)rechten. Der Prozess zur Rechtevergabe ist dokumentiert.
- Die Zugriffsrechte auf verschiedene interne Systeme wird in regelmäßigen Audits überprüft.
- Besonders schützenswerte personenbezogene Daten werden zusätzlich verschlüsselt.
- Der Umgang mit diesen Daten ist in einer Sicherheitsrichtlinie zum Umgang mit klassifizierten Informationen und Datenträgern beschrieben.

I.4. Weitergabekontrolle

- Außer zum Zwecke der Datensicherung erfolgt die Weitergabe personenbezogener Daten nur auf explizite Anweisung durch den Kunden (schriftlicher Change-Request oder Auftrag).
- Im Rahmen der Auslagerung von Sicherungsmedien werden diese Medien transportgesichert. Diese befinden sich in einem getrennten Gebäude. Der Zutritt zu dem dort befindlichen Serverraum ist nur wenigen Mitarbeitern gestattet.
- Die Büroräumlichkeiten und der Serverraum verfügen über eine elektronische Zutrittskontrolle wie in I.1. geschildert. Der Prozess zur Rechtevergabe ist dokumentiert.
- Die Daten sind durch Firewalls und Virenschutzsysteme vor dem Zugriff von außen, sowie Manipulationen, geschützt.
- Bei Transport personenbezogener Daten nach außen werden diese immer verschlüsselt. Die Sicherheitsrichtlinie zum Umgang mit klassifizierten Informationen und Datenträgern enthält weitere Angaben zu den integrierten Maßnahmen zur Kontrolle der Weitergabe von Daten.
- Für die Vernichtung von Dokumenten mit personenbezogenen Daten in Papierform sind Container aufgestellt. Der Zugriff auf die in den Containern enthaltenen Unterlagen/Daten ist nach Einwurf nicht mehr möglich. Diese Dokumente werden durch einen Dienstleister, unter Wahrung der datenschutzrechtlichen Regelungen vernichtet.

I.5. Eingabekontrolle

- Zur Gewährleistung der Eingabekontrolle sind Protokollierungs- und Protokollauswertungs-systeme integriert.
- Das Nachverfolgen von Dateneingaben wird, wo technisch möglich, durch das etablierte Logging-Verfahren gewährleistet. Somit ist es jederzeit nachvollziehbar welche User Daten eingegeben haben.

I.6. Auftragskontrolle

- Generelle Weisungen des Kunden werden zum Zeitpunkt der Vertragsunterschrift in Form einer Einzelvereinbarung dokumentiert und den zuständigen Mitarbeitern im Rahmen einer Einweisung in der Setup-Phase bekannt gemacht. Dort werden auch explizit die Weisungsbefugnisse und Kontrollrechte des Kunden schriftlich festgesetzt.
- Weitere Aufträge des Kunden (z.B. Übertragung von Daten) unterliegen dem Change-Request-Verfahren und werden somit schriftlich dokumentiert.
- Kenntnisse über die Nicht-Einhaltung der Vorgaben des Kunden sind dem Datenschutz-beauftragten zur Kenntnis zu bringen.
- Subunternehmer werden den Vorgaben des § 11 BDSG entsprechend ausgewählt und verpflichtet. Dabei werden Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt. In jedem Einzelfall überzeugt sich der Rechenzentrumsbetreiber vor Beginn der Datenverarbeitung und sodann durch regelmäßige Kontrollen von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen.

I.7. Verfügbarkeitskontrolle

- Grundsätzlich werden alle Systeme, die im Zusammenhang mit der Verarbeitung von personenbezogenen Daten genutzt werden, im Rahmen des Backup-Dienstes regelmäßig gesichert und die Konsistenz der Sicherung wird geprüft.

- Datensicherungsmedien werden in einem getrennten Gebäude aufbewahrt. Der Prozess zur Gewährung von Zutritt folgt dem in I.4. und I.1. dargestellten Ablauf.
- Für Festplattensysteme an Servern werden RAID-Mechanismen eingesetzt, die die Ausfallsicherheit erhöhen.
- Alle Systeme werden über die USVen in den Rechenzentren gegen Spannungsspitzen, Spannungsschwankungen und Unterbrechung der Stromversorgung abgesichert.
- Das Rechenzentrum verfügt über ein Notstromaggregat und redundant ausgelegten Klimaanlagen.
- Brandsensoren überwachen das Rechenzentrum rund um die Uhr.
- Die Verfügbarkeit der Systeme wird mithilfe eines Monitoringtools (Nagios) überwacht.
- Die Infrastruktur wie Backbone, USVen, Strom und Klimaanlagen werden ebenfalls mit dem Nagios-Monitoringtool überwacht.
- Auf den Systemen werden regelmäßig Patches installiert. Der Patch- und Schwachstellen-prozess ist in einer Sicherheitsrichtlinie „Security Prozesse“ dokumentiert.
- Die Daten sind durch Firewalls und Virenschutzsysteme vor dem Zugriff und Manipulation von außen geschützt.

I.8. Trennungskontrolle

- Datensicherungen und Produktivdaten werden getrennt voneinander aufbewahrt.
- Daten von Test- und Produktivsystemen werden getrennt voneinander abgelegt.
- Das Netz ist in verschiedene VLANs gegliedert und dadurch Mandantenfähig.
- Logdateien werden auf einem eigenen Log-System gespeichert.

Abschnitt II: Büroräume billwerk

II.1. Zutrittskontrolle

- Zutritt zu den Büroräumen haben grundsätzlich nur Mitarbeiter von billwerk.
- Gäste müssen sich am Empfang anmelden und dürfen sich nicht unbegleitet im Büro bewegen.
- Zutritt zu den Betriebsräumen ist nur mit Sicherheitsschlüssel oder Magnetkarte möglich.
- Türen, Tore und Fenster sind außerhalb der Betriebszeiten fest verschlossen.

II.2. Zugangskontrolle

- Pro Benutzer wird eine individuelle Benutzerkennung vergeben.
- Passworte werden ausschließlich vom Benutzer erstellt.
- Passworte müssen aus mindestens 8 Zeichen bestehen und mindestens ein Sonderzeichen und/oder eine Zahl enthalten.
- Geräte, von denen aus Zugriff auf Systeme besteht, auf denen Kundendaten gespeichert sind, verfügen über eine automatische Bildschirmsperre bei Inaktivität des Nutzers.

II.3. Zugriffskontrolle

- Individuelle Zuweisung von Rechten pro Benutzer (Abgestufte Zugriffsberechtigung).
- Organisatorische Berechtigungsbewilligung und technische Berechtigungsvergabe erfolgen durch verschiedene Personen.
- Zugriff auf Systeme mit Kundendaten haben nur ausgewählte Mitarbeiter, die einen solchen Zugriff für Ihre Tätigkeit zwingend benötigen.

II.4. Weitergabekontrolle

- Alle Mitarbeiter sind gemäß § 5 BDSG auf das Datengeheimnis verpflichtet.
- Zugriffe auf Daten im Rechenzentrum erfolgen ausschließlich über verschlüsselte Verbindungen.

II.5. Eingabekontrolle

- Jede Eingabe oder Änderung von Kundendaten wird protokolliert.
- Jede Administratortätigkeit (z.B. Anlegen oder Löschen von Benutzern, Änderungen der Benutzerrechte) wird protokolliert (Syslog).

II.6. Auftragskontrolle

- Alle Mitarbeiter werden regelmäßig zum Datenschutz geschult.
- Arbeitsanweisungen werden in Schrift- oder Textform dokumentiert.

II.7. Verfügbarkeitskontrolle

- Keine Maßnahmen erforderlich, da die Datenverarbeitung ausschließlich im Rechenzentrum erfolgt.

II.8. Trennungskontrolle

- Daten, die zu unterschiedlichen Zwecken erhoben wurden werden logisch getrennt voneinander gespeichert.