Nutzername:

zugestimmt am:

zwischen:

	Und	**Bundesanzeiger Verlag GmbH** **Amsterdamer Str. 192** **50735 Köln**
-nachfolgend „Auftraggeberin“ genannt-		-nachfolgend „Auftragnehmerin“ genannt

Der Datenverarbeitung liegt der im Rahmen der Nutzung von eBilanz-Online zwischen Auftraggeberin und Auftragnehmerin abgeschlossene Vertrag zu Grunde.

§ 1 Gegenstand der Vereinbarung

Die Auftragnehmerin stellt der Auftraggeberin im Rahmen von IT-Dienstleistungen die Anwendung **eBilanz-Online** zur Verfügung.

eBilanz-Online ist eine webbasierte Anwendung zur Unterstützung des Erfassungs- und Übertragungsprozesses im Rahmen der gesetzlichen Anforderungen des § 5b EStG zur elektronischen Übertragung von Bilanzen sowie Gewinn- und Verlustrechnungen (sog. E-Bilanz). Darüber hinaus kann sie auch zur Erstellung einer XBRL-Datei verwendet werden, mit der die handelsrechtliche Offenlegung des Jahresabschlusses im Bundesanzeiger erfolgen kann. Zudem ist die Übermittlung eines handelsrechtlichen Jahresabschlusses an Kreditinstitute und Rating-Agenturen zur Bonitätsprüfung (Digitaler Finanzbericht / DiFin) möglich.

Diese Vereinbarung regelt die datenschutzrechtlichen Rechte und Pflichten des zu Grunde liegenden Vertragsverhältnisses. Eine weitergehende Beschreibung zu Umfang, Art und Zweck der Dienstleistung findet sich in **Anlage 1** zu dieser Vereinbarung.

Dazu verarbeitet die Auftragnehmerin personenbezogene Daten im Auftrag der Auftraggeberin, sogenannte „Auftragsverarbeitung (AVV)“. Dieser Auftrag umfasst die im zu Grunde liegenden Auftragsverhältnis vereinbarten Verarbeitungstätigkeiten. Die Inhalte dieses Vertrags gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verarbeitungen im Auftrag vorgenommen wird, und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

§ 2. Definitionen

Die in dieser Auftragsverarbeitungsvereinbarung verwendeten Begriffe richten sich im Zweifel nach dem Gesetz. Lediglich zu Erläuterung einiger Begrifflichkeiten dieses Vertrages erfolgen die folgenden Definitionen:

„Auftraggeberin“ bezeichnet auch einen Verantwortlichen i.S.d. Art. 4 Nr. 7 DSGVO.

„Auftragnehmerin“ bezeichnet auch einen Auftragsverarbeiter i.S.d. Art. 4 Nr. 8 DSGVO.

„Verantwortlicher“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.

„Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung, die Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich, die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

§ 3 Pflichten der Auftraggeberin

(1) Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist die Auftragnehmerin verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftra ggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

(2) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeberin und Auftragnehmerin abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

(3) Die Auftraggeberin hat das Recht, Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Sie erteilt alle Aufträge, Teilaufträge und Weisungen schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen. Bei einem Wechsel oder einer längerfristigen Verhinderung des Anspre chpartners ist der Auftraggeberin unverzüglich schriftlich eine Nachfolgerin bzw. eine Vertreterin mitzuteilen.

   Weisungsempfangende Personen der
   Auftragnehmerin: Die Geschäftsführer und
   Herr Sascha Heinig, Herr Martin Jäger

(4) Die Auftraggeberin informiert die Auftragnehmerin unverzüglich, wenn Fehler oder Unregelmäßigkeiten und etwaige Mängel bezüglich datenschutzrechtlicher Bestim mungen bei der Prüfung der Auftragsergebnisse festgestellt werden. Die Auftra gnehmerin informiert die Auftraggeberin unverzüglich, falls sie der Auffassung ist, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

(5) Die Auftraggeberin und die Auftragnehmerin führen eigene Dokumentationen. Soweit gesetzlich zulässig, kann die Dokumentationspflicht in einer gleichwertigen Betrie bsvereinbarung abgebildet werden. Die Parteien unterstützen sich, soweit erforderlich,

im Rahmen ihrer Möglichkeiten, gegenseitig bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten.

§ 4 Pflichten der Auftragnehmerin

(1) Die Auftragnehmerin verarbeitet personenbezogene Daten für die Auftraggeberin im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO ausschließlich im Rahmen auf Grundlage dieses Vertrages. Sie verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen Zwecke. Kopien oder Duplikate werden ohne Wissen der Auftraggeberin nicht erstellt.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten, spätestens mit Ende der dieser Vereinbarung zu Grunde liegenden Verarbeitung hat die Auftragnehmerin sämtliche in ihrem Besitz gelangten Unterlagen und erstellten Verarbeitungs- und Nutzun gsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverh ältnis stehen, datenschutzgerecht zu vernichten. Test- und Ausschussmaterial ist ebenfalls unverzüglich zu vernichten oder der Auftraggeberin auszuhändigen. Hiervon ausgenommen sind Daten und Informationen welche die Auftragnehmerin aufgrund gesetzlicher Archivierungsfristen nicht löschen kann oder darf.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Verarb eitung personenbezogener Daten dienen, sind durch die Auftragnehmerin entspr echend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

(4) Die Auftragnehmerin bestätigt, dass sie - soweit sie gesetzlich dazu verpflichtet ist (Art. 37 DSGVO) - eine/n Datenschutzbeauftragte/n bestellt hat. Auf Anfrage teilt die Auftragnehmerin die Kontaktdaten des/der Datenschutzbeauftragten - oder soweit ein solcher nicht zu bestellen ist, einer für den Datenschutz bei der Auftragnehmerin verantwortlichen Person - mit.

(5) Die Auftragnehmerin verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten der Auftraggeberin das Datengeheimnis nach Art. 5 DSGVO und § 53 BDSG zu wahren und Daten nur im Rahmen des vertraglich festgesetzten und gesetzlich erlaubten Zweckes zu verarbeiten.

(6) Die Auftragnehmerin sichert zu, dass sie die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet hat.

(7) Die Auftragnehmerin unterstützt die Auftraggeberin, insbesondere durch Bereitstellung entsprechender Informationen bei den gesetzlichen Pflichten der Risikoabschätzung sowie der Vorabkontrolle bzw. Datenschutzfolgenabschätzung. Die angemessenen Kosten der Unterstützung werden von der Auftraggeberin erstattet.

(8) Ist die Auftraggeberin aufgrund geltender Datenschutzgesetze gegenüber einer Einzel person verpflichtet, Auskunft zur Verarbeitung von Daten dieser Person zu geben,

wird die Auftragnehmerin die Auftraggeberin dabei unterstützen, diese Informationen bereit zu stellen, auch durch geeignete technisch-organisatorische Maßnahmen.

(9) Um die Synchronisierung und Überprüfbarkeit der technischen und organisatorischen Maßnahmen zu vereinfachen, richten diese sich insbesondere nach der Anlage 2 zu dieser Vereinbarung die als verbindlich vereinbarter Mindeststandard anzusehen und regelmäßig zu aktualisieren ist.

§ 5 Kontrollrechte

(1) Die Auftraggeberin oder ein im Einzelfall von der Auftraggeberin nachweislich legitimierter zu benennender Prüfer können sich nach angemessen rechtzeitiger Anmeldung zu Prüfzwecken zu den üblichen Geschäftszeiten ohne Störung des Betrie bsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der technischen und organisatorischen Erfordernisse der für die Auftragsverarbeitung einschlägigen Datenschutzgesetze überzeugen. Während der Laufzeit des Auftrags stellt die Auftra gnehmerin sicher, dass sich die Auftraggeberin von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Die angeme ssenen Kosten für die Mitwirkung bei einer solchen Prüfung auf Seiten der Auftra gnehmerin werden von der Auftraggeberin erstattet.

(2) Die Auftragnehmerin verpflichtet sich, der Auftraggeberin auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu geben, die zur Durchführung einer umfassenden Auftragskontrolle erforderlich sind. Die angemessenen Kosten für die Mitwirkung bei einer solchen Prüfung auf Seiten der Auftragnehmerin werden von der Auftraggeberin erstattet.

§ 6 Subunternehmer

(1) Die Auftraggeberin ist damit einverstanden, dass die Auftragnehmerin zur Erfüllung ihrer vertraglich vereinbarten Leistungen kooperierende Unternehmen zur Leistungserf üllung heranzieht bzw. Unternehmen mit Leistungen unterbeauftragt. Im Fall einer beabsichtigten Hinzuziehung oder Ersetzung eines Subunternehmers, wird die Auftra gnehmerin die Auftraggeberin informieren und ihr Gelegenheit zum Einspruch geben. Die Zustimmung zu folgenden Unterauftragnehmern gilt hiermit als erteilt:
   (a) PlusServer GmbH, Welserstraße 14, 51149 Köln
   (b) fwsb GmbH, Hauptstraße 221, 65760 Eschborn

(2) Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftra ggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standa rdklauseln („standard-clauses“), genehmigte Verhaltensregeln).

§ 7 Unrechtmäßige Kenntniserlangung von Daten durch Dritte - Datenpannen und Störungen

Die Auftragnehmerin teilt der Auftraggeberin unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Kenntniserlangung, sämtliche Verletzungen des Schutzes personenbezogener Daten, Störungen, Verstöße der Auftragnehmerin oder der bei ihr beschäftigten oder von ihr beauftragten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen mit.

§ 8 Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO (Art. 28 Abs. 3 Satz 2 lit. c DSGVO)

Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DSGVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird. Die in **Anlage 2** beschriebene Dokumentation stellt die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragnehmer dar.

§ 9 Dauer der Vereinbarung

(1) Der Vertrag beginnt mit letzter Unterschrift durch die Auftragnehmerin und der Auftra ggeberin und richtet sich nach der Dauer der Datenverarbeitung.
(2) Beide Vertragspartner können den Auftrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß gegen die anzuwendenden Datens chutzvorschriften vorliegt. Als Grund ausgenommen sind Weisungen und Verlangen, die gegen geltendes Recht verstoßen.

§ 10 Sonstiges

(1) Änderungen und Ergänzungen dieses Vertrages bedürfen einer Vereinbarung in gleicher Form 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.
(2) Auf den Vertrag ist das Recht der Bundesrepublik Deutschland anzuwenden. Die Sprache des Verfahrens ist Deutsch. Der Gerichtsstand ist, soweit es gesetzlich zulässig ist, dies durch diese Vereinbarung zu regeln, Köln.
(3) Sollte eine Bestimmung dieses Vertrages unwirksam oder undurchführbar sein oder werden, so berührt dies, unter Ausschluss von § 139 BGB, nicht die Wirksamkeit

des Vertrages im Übrigen. Dies soll keine Beweislastumkehr bewirken, sondern § 139 BGB wird ausdrücklich abbedungen. Anstelle der unwirksamen oder undurchführbaren Bestimmung oder zur Ausfüllung eventueller Lücken soll eine angemessene Regelung gelten, die - soweit rechtlich möglich - dem am nächsten kommt, was die Vertragspartner nach dem Sinn des Vertrages gewollt haben.

Anlagen:

1 „Datenblatt“
2 technische und organisatorische Maßnahmen („TOM“)

Köln Bundesanzeiger Verlag GmbH

Anlage 1 zur Vereinbarung zur Auftragsdatenverarbeitung - **Datenblatt**

1. Gegenstand und Dauer der Auftragsverarbeitung

1.1. Der Gegenstand der Auftragsverarbeitung ergibt sich aus dieser Vereinbarung zur Auftrasgsverarbeitung und dem zu Grunde liegenden Auftragsverhältnisses.

1.2 Der Umgang mit den Daten der Betroffenen durch die Auftragnehmerin erfolgt technisch in Systemen:

- der Auftragnehmerin
- Eines Dritten
  (fwsb GmbH, PlusServer GmbH)

1. Art der personenbezogenen Daten entsprechend der Definition von Art. 4 Nr. 1, 13, 14 und 15 DSGVO

- Vor- und Zuname
- Geburtsname
- Kunden-/Mitarbeiter-nummer/Identifikations-Nr.
- Passwörter (verschlüsselt)
- Telefon-/Faxnummer
- E-Mail-Adresse(n)
- Bankverbindung (IBAN, BIC, Bank)
- Steuerdaten

2. Kreis der Betroffenen (entsprechend der Definition von Art. 4 Nr. 1 DSGVO)

- Kunden der Auftraggeberin
- Mitarbeiter der Auftraggeberin
- Mitarbeiter der Auftragnehmerin

3. Löschung, Sperrung und Berichtigung von Daten:

Die erhaltenden Daten gem. Anlage 1 Nr. 1 sind zu löschen

- nach Abschluss der Dienstleistung und Ablauf einschlägiger gesetzlicher Aufbewahrungsfristen

Nach erfolgter Löschung bzw. Vernichtung ist die Auftraggeberin hierüber umgehend schriftlich in Kenntnis zu setzen.
Die Löschung der Daten erfolgt durch:

- Löschkommandos des jeweiligen Betriebssystems

4. Kontaktdaten der Datenschutzbeauftragten:

Für die Auftragnehmerin:	
Name (Fam., Vor.):	Freund, Gesine und Stiens, Ursula
Funktion:	Datenschutzbeauftragte
Anschrift:	Amsterdamer Str. 192,50735 Köln
E-Mail:	dsb@bundesanzeiger.de

Anlage 2 zur Vereinbarung zur Auftragsdatenverarbeitung
- **technische und organisatorische Maßnahmen („TOM“)**

Der Auftragnehmer verpflichtet sich ein Datenschutz- und Datensicherheitskonzept vorzuhalten. Dieses umfasst die nachfolgend dargestellten und technischen und organisatorischen Maßnahmen, als Mindeststandard, die vom Auftragnehmer auf seine Kosten durchzuführen und zu erhalten sind, vgl Art. 32 Abs. 1 DSGVO.

Anforderungen an die Sicherheit der Datenverarbeitung gemäß Art. 32 DSGVO, § 64 BDSG

1. Risikoanalyse nach Art. 32 DSGVO

Schutzbedarf der personenbezogenen Daten:
Der Schutzbedarf wird im Hinblick auf die betroffenen Datenkategorien und betroffenen Personengruppen ermittelt.
Mögliche und berücksichtigte Risiken für die personenbezogenen Daten

- Verlust von Daten zum Beispiel durch Löschung
- Zugriff durch unbefugte Dritte
- Veränderung von Daten durch den Auftragnehmer

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

2.1 Zugangskontrolle

Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (Zugangskontrolle).

Technische Maßnahmen
Organisatorische Maßnahmen

- Alarmanlage
- Chipkarten-/Transponder-Schließsystem
- Manuelles Schließsystem
- Eingezäuntes Gebäude
- Regelmäßige Kontrollrundgänge

- Personenkontrolle beim Pförtner/Empfang
- Protokollierung der Besucher/Besucherbuch
- Schlüsselregelung/Schlüsselbuch
- Sorgfältige Auswahl von Sicherheitspersonal
- Tragepflicht von Mitarbeiter-/Gästeausweisen
- Videoüberwachung der Zugänge
- Abgegrenzte Serverräume mit folgenden Zutrittsbeschränkungen:
  (Schlüsselregelung, Codekarte)

2.2 Datenträger- Benutzerkontrolle

Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern (Datenträgerkontrolle) und

Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (Benutzerkontrolle)

Technische Maßnahmen
Organisatorische Maßnahmen

- Authentifikation mit Benutzer+Passwort
- Einsatz von Anti-Viren-Software
- Einsatz von Firewalls
- Einsatz von Mobile Device Management
- Einsatz von VPN-Technologie
- Sperren von externen Schnittstellen (z. B. USB-Anschlüsse)
- Weitere:
  (SSL-Verschlüsselung)

- Benutzerberechtigungen verwalten
- Passwortvergabe/Passwortregeln
- Passworthistorie
- Protokollierung der Besucher/Besucherbuch

- Schlüsselregelung/Schlüsselbuch
- Sorgfältige Auswahl von Reinigungspersonal
- Systemadministration durch:
  (Getrennte Benutzerkonten für Systemadministration, Sachbearbeitung, persönlichen Nutzungen)

2.3 Zugriffs- und Eingabekontrolle

Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben.

Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind (Eingabekontrolle).

Technische Maßnahmen
Organisatorische Maßnahmen

- Einsatz von Aktenvernichtern
- Ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)
- Protokollierung der Vernichtung von Daten
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Verschlüsselung von Smartphones
- Regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik)
- Zugriffsschutz durch Bildschirmschoner - Aufhebung nur mit Passwort
- Clean-Desk und Clean-Screen Richtlinie

- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Einsatz von Dienstleistern zur Akten- und Datenvernichtung (nach Möglichkeit mit Zertifikat)
- Erstellen eines Berechtigungskonzepts und Ausgestaltung der Zugriffsrechte
- Passwortrichtlinie inkl. Länge und Wechsel
- Verwaltung der Benutzerrechte durch Systemadministratoren
- Sichere Aufbewahrung von Datenträgern
- Erfassung und Protokollierung der verwendeten Datenträger

2.4 Trennbarkeit

Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können (Trennbarkeit).

Technische Maßnahmen
Organisatorische Maßnahmen

- Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Trennung von Produktiv- und Testsystem
- Logische Mandantentrennung (softwareseitig)

- Erstellung eines Berechtigungskonzepts
- Festlegung von Datenbankenrechten
- Trennung zwischen der Verarbeitung von Produktions- und Testdaten
- Trennung Bankdaten von Passwörtern von sonstigem Nutzer- und Zugangsdaten

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

3.1 Übertragungs- und Transportkontrolle

Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle).

Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden (Transportkontrolle).

Technische Maßnahmen
Organisatorische Maßnahmen

- Einrichtungen von VPN-Tunneln
- E-Mail-Verschlüsselung
- Verschlüsselte Datenübertragung
- Festplattenverschlüsselung (mobile Arbeitsgeräte)

- Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- Protokolle und Regelungen für Fernwartung
- Verpflichtung d. Mitarbeiter auf das Datengeheimnis

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

4.1 Verfügbarkeits- und Zuverlässigkeitskontrolle

Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle).

Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit).

Technische Maßnahmen
Organisatorische Maßnahmen

- Feuerlöschgeräte in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Klimaanlage in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Unterbrechungsfreie Stromversorgung (USV) oder Generator
- In Hochwassergebieten: Serverräume über der Wassergrenze
- Datensicherungsverfahren
  Spiegeln der Festplatten (z.B. RAID)
- Intrusion Detection System (IDS) / Intrusion Prevention System (IPS)
- Spam-Filter

- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Backup- und Recoverykonzepts mit täglicher Sicherung der relevanten Daten
- Erstellen eines Notfallplans
- Testen von Datenwiderherstellung
- Serverräume nicht unter sanitären Anlagen
- Notfallplan

4.2 Belastbarkeit

Technische Maßnahmen
Organisatorische Maßnahmen

- Alle Systeme sind durch redundante Firewall-Systeme vor Angriffen geschützt

- Bei Erreichen eines Auslastungsgrads des permanenten Speichers (Storage) > als die definierten Schwellwerte wird das Gesamtsystem durch Hinzufügen weiterer Ressourcen oder Entlastung der alten (z.B. Löschen alter Bestände) wieder entlastet

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

5.1 Datenschutzmanagement und Integrität bei der Datenverarbeitung

Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität).

Technische Maßnahmen
Organisatorische Maßnahmen

- Alle Systeme sind durch redundante Firewall-Systeme vor Angriffen geschützt

- Bei Erreichen eines Auslastungsgrads des permanenten Speichers (Storage) > als die definierten Schwellwerte wird das Gesamtsystem durch Hinzufügen weiterer Ressourcen oder Entlastung der alten (z.B. Löschen alter Bestände) wieder entlastet

5.2 Auftragskontrolle

Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:

- Auswahl der Auftragnehmerin unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- Verpflichtung der Mitarbeiter der Auftragnehmerin auf das Datengeheimnis
- Regelmäßige Unterweisung der Mitarbeiter im Datenschutzrecht