

Datenschutzvereinbarung

zwischen dem

Gemeinsamer Bundesausschuss (GBA),
Gutenbergstraße 13
10587 Berlin

- Verantwortlicher - nachstehend Auftraggeber genannt -
und dem/der

.....
- Auftragsverarbeiter - nachstehend Auftragnehmer genannt
[ggf.: Vertreter gemäß Art. 27 DSGVO:
.....

Inhalt

Datenschutzvereinbarung	1
Präambel	2
1. Gegenstand und Dauer des Auftrags	2
2. Konkretisierung des Auftragsinhalts	2
3. Technisch-organisatorische Maßnahmen	3
4. Berichtigung, Einschränkung, Löschung und Rückgabe von Daten.....	4
5. Umsetzung Betroffenenrechte.....	5
6. Qualitätssicherung und sonstige Pflichten des Auftragnehmers	5
7. Unterauftragsverhältnisse.....	7
8. Kontrollrechte des Auftraggebers	8
9. Mitteilung bei Verstößen des Auftragnehmers.....	9
10. Weisungsbefugnis des Auftraggebers	9
11. Zurückbehaltungsrecht.....	10
12. Haftung.....	10
[OPTIONAL:] 13. Fernzugriff bei Prüfungen/Wartungen eines Systems oder anderen Dienstleistungen über Fernzugriffe.....	10
I. Anlage – Technisch-organisatorische Maßnahmen	12

Präambel

Der Auftragnehmer ist Auftragsverarbeiter gemäß der Datenschutzgrundverordnung („DSGVO“). Als Anlage zu dem zwischen ihnen geschlossenen Vertrag über Druck- und Versandleistungen der Versicherteninformationen und Untersuchungshefte vom DD.MM.YYYY (nachfolgend auch „Hauptvertrag“ genannt) schließen die Vertragspartner diesen Auftragsverarbeitungs-Vertrag („AV-Vertrag“).

Dieser AV-Vertrag unterliegt den Bestimmungen der DSGVO und dem Bundesdatenschutzgesetz („BDSG“) in seiner jeweils gültigen Fassung. Die Bestimmungen dieses Vertrags gehen im Kollisionsfalle hinsichtlich der Verwendung personenbezogener Daten i.S.d. DSGVO und BDSG den Bestimmungen des Hauptvertrages vor.

Sämtliche in diesem AV-Vertrag beschriebenen Verpflichtungen finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen Mitarbeiterinnen und Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen bzw. kommen können.

Der Auftragnehmer ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebsgeheimnissen und Datensicherheitsmaßnahmen des Auftraggebers vertraulich zu behandeln.

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Der Gegenstand des Auftrags ergibt sich aus dem Hauptvertrag, auf den hier verwiesen wird.

(2) Dauer

Die Laufzeit dieses Vertrages richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den Bestimmungen dieses AV-Vertrages nicht etwas Anderes ergibt.

Es ist den Vertragspartnern bewusst, dass ohne Vorliegen eines gültigen AV-Vertrages z. B. bei Beendigung des vorliegenden Vertragsverhältnisses, keine (weitere) Auftragsverarbeitung durchgeführt werden darf.

Das Recht zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt. Kündigungen bedürfen zu ihrer Wirksamkeit der Schriftform.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Umfang, Art und Zweck der Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten sind im Hauptvertrag enthalten.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

(2) Art der Daten

Für die Leistungserbringung nach dem Hauptvertrag und seiner Anlagen folgende Datenarten/-kategorien Gegenstand der Verarbeitung:

- ☒ Personenstammdaten (z.B. Name, Anschrift, Geburtsdaten)
- ☒ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☒ Kundenhistorie
- ☒ Vertragsabrechnungs- und Zahlungsdaten
- ☐ Planungs- und Steuerungsdaten
- ☐ Auskunftangaben (von Dritten, z.B. Auskunftsteilen, oder aus öffentlichen Verzeichnissen)
- ☐ Bank-, Finanz- und Steuerdaten (z.B. Vermögen, Verbindlichkeiten, Einkommen, Verpflichtungen oder vergleichbare Daten)
- ☐ Besondere Kategorien von Daten(arten) (z.B. rassische oder ethnische Herkunft, religiöse Überzeugung, weltanschauliche (philosophische) Überzeugung, politische Überzeugungen/ Meinungen, Gesundheit (inkl. genetischer Daten), Biometrischen Daten zur (eindeutigen) Identifizierung einer Person, Gewerkschaftszugehörigkeit, Sexualleben oder der sexuellen Orientierung)
- ☐

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ☒ Kunden des Auftraggebers
- ☐ Interessenten
- ☐ Abonnenten
- ☒ Beschäftigte
- ☒ Lieferanten
- ☐ Handelsvertreter
- ☒ Ansprechpartner
- ☐

3. Technisch-organisatorische Maßnahmen

(1) 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 zur angemessenen Sicherung der Daten des Auftraggebers vor Missbrauch und Verlust treffen, die den Anforderungen der entsprechenden datenschutzrechtlichen Bestimmungen entsprechen; diese Maßnahmen muss der Auftragnehmer auf Anfrage dem Auftraggeber und ggfs. Aufsichtsbehörden gegenüber nachweisen.

(2) 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.

(3) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 litt. 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 1].

(4) 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.

(5) Der Auftragnehmer stellt dem Auftraggeber auf dessen Wunsch ein aussagekräftiges und aktuelles Datenschutz- und Sicherheitskonzept für diese Auftragsverarbeitung zur Verfügung.

4. Berichtigung, Einschränkung, Löschung und Rückgabe 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.

(2) 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.

(3) 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.

(4) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung des Hauptvertrages – 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.

(5) 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.

(6) 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 Verantwortlichen im Sinne der DSGVO liegen.

(7) Sofern eine Vernichtung während der laufenden Beauftragung vorzunehmen ist, übernimmt der Auftragnehmer die nachweislich datenschutzkonforme Vernichtung von Datenträgern und sonstiger Materialien nur aufgrund entsprechender Einzelbeauftragung durch den Auftraggeber.

(8) Auch bei Störungen im Betriebsablauf, etwa bei Hardwareaustausch, hat der Auftragnehmer dafür Sorge zu tragen, dass keine Daten des Auftraggebers an Dritte weitergegeben bzw. dass Daten auf der auszutauschenden Hardware vor der Weitergabe unwiederbringlich gelöscht werden. Der Auftragnehmer garantiert dem Auftraggeber die ordnungsgemäße Vernichtung jedes nicht benötigten Datenmaterials (Probeausdrucke, überzählige Listen etc.). Zu entsorgende Unterlagen sind mit dem Aktenvernichter nach DIN 32757-1 mindestens Stufe 3 unleserlich zu machen oder in einer dafür vorgesehenen „Datenschutztonne“. Sollte eine höhere Stufe erforderlich sein, teilen sich dies die Vertragspartner jeweils mit.

(9) Sofern zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten entstehen, bedarf es einer vorherigen schriftlichen Vereinbarung über die Kostentragung.

(10) Soweit ein Transport des Speichermediums vor Löschung unverzichtbar ist, wird der Auftragnehmer angemessene Maßnahmen zu dessen Schutz, insbesondere gegen Entwendung, unbefugtem Lesen, Kopieren oder Verändern, treffen. Die Maßnahmen und die anzuwendenden Löschverfahren werden bei Bedarf ergänzend zu den Leistungsbeschreibungen konkretisierend vereinbart.

5. Umsetzung Betroffenenrechte

(1) Soweit eine betroffene Person sich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

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

(3) Der Auftragnehmer wird dem Auftraggeber durch Bereitstellung der entsprechenden Informationen unterstützen, wenn der Auftraggeber auf Grund von Datenschutzrecht verpflichtet ist, einem Betroffenen Auskünfte zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten dieser Person zu erteilen, und wenn der Auftraggeber den Auftragnehmer hierzu schriftlich, mindestens via Email, auffordert.

6. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

(1) Als Datenschutzbeauftragter gemäß Art. 37 ff. DSGVO, ist beim Auftragnehmer derzeit **Name, Kontaktdaten** benannt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich schriftlich mitzuteilen. Der Auftragnehmer gewährleistet, dass die Anforderungen an den Datenschutzbeauftragten und seine Tätigkeit gemäß Art. 38 DSGVO erfüllt werden.

[optional] Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird Herr/Frau [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail] benannt.

[optional] Da der Auftragnehmer seinen Sitz außerhalb der Union hat, benennt er folgenden Vertreter nach Art. 27 Abs. 1 DSGVO in der Union: [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail].

(2) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 litt. b, 29, 32 Abs. 4 DSGVO. 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 Art. 28 Abs. 3 S. 2 litt. c, 32 DSGVO [Einzelheiten in Anlage 1].

(4) Der Auftraggeber und der 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.

(8) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

(9) Der Auftragnehmer ist bzgl. der zu verarbeitenden Daten für die Einhaltung der jeweils für sich einschlägigen Datenschutzgesetze verantwortlich.

(10) Der Auftragnehmer selbst führt für die Verarbeitung ein Verzeichnis der bei ihm stattfindenden Verarbeitungstätigkeiten im Sinne des Art. 30 DSGVO. Er stellt auf Anforderung dem Auftraggeber die für die Übersicht nach Art. 30 DSGVO notwendigen Angaben zur Verfügung. Des Weiteren stellt er das Verzeichnis auf Anfrage der Aufsichtsbehörde zur Verfügung.

(11) Der Auftragnehmer unterstützt den Auftraggeber bei der Datenschutzfolgenabschätzung mit allen ihm zur Verfügung stehenden Informationen. Im Falle der Notwendigkeit einer vorherigen Konsultation der zuständigen Aufsichtsbehörde unterstützt der Auftragnehmer den Auftraggeber auch hierbei.

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.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

(3) Zum Zeitpunkt des Abschlusses dieser Vereinbarung werden die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Leistungsteile unter Einschaltung eines Unterauftragnehmers durchgeführt, nämlich

Firma Unterauftragnehmer	Anschrift/Land	Beschreibung der Teilleistung

(4) Die Auslagerung oder der Wechsel auf/des Unterauftragnehmer(s) oder sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer 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.

(5) Der Auftragnehmer muss Unterauftragnehmer unter besonderer Berücksichtigung der Eignung hinsichtlich der Erfüllung der zwischen Auftraggeber und Auftragnehmer vereinbarten technischen und organisatorischen Maßnahmen gewissenhaft auswählen.

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

(7) Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

(8) Ist der Auftragnehmer im Sinne dieser Vereinbarung befugt, die Dienste eines Unterauftragnehmers in Anspruch zu nehmen, um bestimmte Verarbeitungstätigkeiten im Namen des Auftraggebers auszuführen, so werden diesem Unterauftragnehmer im Wege eines Vertrags dieselben Pflichten auferlegt, die in dieser Vereinbarung zwischen dem Auftraggeber und dem Auftragnehmer festgelegt sind, insbesondere hinsichtlich der Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit zwischen den Vertragspartnern dieses Vertrages sowie den in diesem AV-Vertrag

beschriebenen Kontroll- und Überprüfungsrechten des Auftraggebers. Hierbei müssen ferner hinreichend Garantien dafür geboten werden, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt.

(9) Durch schriftliche Aufforderung ist der Auftraggeber berechtigt, vom Auftragnehmer Auskunft über die datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen.

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.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO 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

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(4) Der Auftraggeber wird den Auftragnehmer informieren, wenn er bei der Prüfung der Auftrags-ergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(5) Die Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch den Auftraggeber im Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags, wird vom Auftragnehmer unterstützt.

(6) Der Auftraggeber kann sich regelmäßig von der Wirksamkeit der beim Auftragnehmer gemäß dieser Vereinbarung getroffenen technischen und organisatorischen Maßnahmen überzeugen. Hierzu kann der Auftraggeber auch geeignete Dritte mit der Prüfung beauftragen. Dem Auftraggeber bzw. beauftragten Dritten ist im Falle einer Vorortkontrolle beim Auftragnehmer durch diesen angemessenen Zutritt zu den datenverarbeitenden Unternehmensbereichen zu gewähren, sowie Auskunft zu erteilen. Anstelle einer Prüfung durch den Auftraggeber oder Dritte kann der Auftragnehmer dem Auftraggeber im Regelfall die Einhaltung der technischen und organisatorischen Maßnahmen gemäß dieser Vereinbarung auch mittels eines Wirtschaftsprüfers-Testats oder eines Zertifikats über ein Sicherheits-/Datenschutzaudit belegen; die Einzelheiten hierzu sind vom Auftragnehmer im Vorwege mit dem Auftraggeber abzustimmen.

(7) Liegt ein Verstoß des Auftragnehmers oder der bei ihm im Rahmen des Auftrags beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder der im Vertrag getroffenen Festlegungen vor, oder bestehen hierfür begründete Anhaltspunkte, so kann eine darauf bezogene Prüfung auch ohne rechtzeitige Anmeldung vorgenommen werden.

9. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei Verstößen des Auftragnehmers oder der bei ihm im Rahmen des Auftrags beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder der im Vertrag getroffenen Festlegungen.

(2) Er trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die Betroffenen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

(3) Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung der Informationspflichten gegenüber der jeweils zuständigen Aufsichtsbehörde bzw. den von einer Verletzung des Schutzes personenbezogener Daten Betroffenen nach Art. 33, 34 DSGVO.

(4) Der Auftragnehmer unterstützt den Auftraggeber 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 Unterstützung des Auftraggebers für dessen Datenschutz-Folgeabschätzung
- die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(5) Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen und Maßnahmen durch die Aufsichtsbehörden oder falls eine Aufsichtsbehörde bei dem Auftragnehmer ermittelt.

(6) Dem Auftraggeber obliegen die aus Art. 33, 34 DSGVO resultierenden Informationspflichten gegenüber der Aufsichtsbehörde bzw. den von einer Verletzung des Schutzes personenbezogener Daten Betroffenen.

10. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform). Der Auftragnehmer notiert sich Datum, Uhrzeit und Person, welche die mündliche Weisung erteilt sowie den Grund, warum keine schriftliche Beauftragung erfolgen konnte.

(2) 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.

(3) Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierter Weisung des Auftraggebers. Ausgenommen hiervon sind Sachverhalte, in denen dem Auftragnehmer eine Verarbeitung aus zwingenden rechtlichen Gründen auferlegt wird. Der Auftragnehmer unterrichtet soweit ihm möglich in derartigen Situationen den Auftraggeber vor Beginn der Verarbeitung über die entsprechenden rechtlichen Anforderungen. Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, dass er durch Einzelweisungen konkretisieren kann.

11. Zurückbehaltungsrecht

Die Einrede des Zurückbehaltungsrechts gleich aus welchem Rechtsgrund, an den vertragsgegenständlichen Daten sowie an evtl. vorhandenen Datenträgern wird ausgeschlossen.

12. Haftung

(1) Auftraggeber und Auftragnehmer haften für den Schaden, der durch eine nicht der DSGVO entsprechende Verarbeitung verursacht wird, gemeinsam im Außenverhältnis gegenüber der jeweiligen betroffenen Person.

(2) Der Auftragnehmer haftet für Schäden, die auf einer von ihm durchgeführten Verarbeitung beruhen, bei der

- er den aus der DSGVO resultierenden und speziell für Auftragsverarbeiter auferlegten Pflichten nicht nachgekommen ist oder
- er unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Auftraggebers handelte oder
- er gegen die rechtmäßig erteilten Anweisungen des Auftraggebers gehandelt hat.

(3) Die Haftung des Auftragnehmers erstreckt sich auch auf entsprechende Verstöße etwaiger Unterauftragnehmer.

(4) Soweit der Auftraggeber zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff auf den Auftragnehmer vorbehalten.

(5) Weitergehende gesetzliche oder vertragliche Haftungsansprüche bleiben unberührt.

[OPTIONAL:] 13. Fernzugriff bei Prüfungen/Wartungen eines Systems oder anderen Dienstleistungen über Fernzugriffe

Für die Durchführung von Fernzugriffen bei der Prüfung und/oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen oder bei Fernzugriffen für andere Dienstleistungen gelten ergänzend folgende Rechte/Pflichten des Auftraggebers/Auftragnehmers:

(1) Fernzugriffe im Rahmen von Prüfungs- und/oder Wartungsarbeiten an Arbeitsplatzsystemen werden erst nach Freigabe durch den jeweiligen Berechtigten / zuständigen Mitarbeiter des Auftraggebers durchgeführt.

(2) Fernzugriffe im Rahmen von Prüfungs- und/oder Wartungsarbeiten von automatisierten Verfahren oder von Datenverarbeitungsanlagen werden, sofern hierbei ein Zugriff auf personenbezogene Daten nicht sicher ausgeschlossen werden kann, ausschließlich mit Zustimmung des Auftraggebers ausgeführt.

(3) Die Mitarbeiter des Auftragnehmers verwenden angemessene Identifizierungs- und Verschlüsselungsverfahren.

(4) Vor Durchführung von Fernzugriffen werden sich Auftraggeber und Auftragnehmer über ggf. notwendige Datensicherheitsmaßnahmen in ihren jeweiligen Verantwortungsbereichen verständigen.

(5) Fernzugriffe im Rahmen von Prüfungs- und/oder Wartungsarbeiten werden dokumentiert und protokolliert. Der Auftraggeber ist berechtigt, Prüfungs- und Wartungsarbeiten vor, bei und nach Durchführung zu kontrollieren. Bei Fernzugriffen ist der Auftraggeber - soweit technisch möglich - berechtigt, diese von einem Kontrollbildschirm aus zu verfolgen und jederzeit abubrechen.

(6) Der Auftragnehmer wird von den ihm eingeräumten Zugriffsrechten auf automatisierte Verfahren oder von Datenverarbeitungsanlagen (insb. IT-Systeme, Anwendungen) des Auftraggebers nur in dem Umfang - auch in zeitlicher Hinsicht - Gebrauch machen, wie dies für die ordnungsgemäße Durchführung der beauftragten Wartungs- und Prüfungsarbeiten notwendig ist.

(7) Soweit bei der Leistungserbringung Tätigkeiten zur Fehleranalyse erforderlich sind, bei denen eine Kenntnisnahme (z. B. auch lesender Zugriff) oder ein Zugriff auf Wirkdaten (Produktions-/Echtdaten) des Auftraggebers notwendig ist, wird der Auftragnehmer die vorherige Einwilligung des Auftraggebers einholen.

(8) Tätigkeiten zur Fehleranalyse, bei denen ein Datenabzug der Wirkbetriebsdaten erforderlich ist, bedürfen der vorherigen Einwilligung des Auftraggebers. Bei Datenabzug der Wirkbetriebsdaten wird der Auftragnehmer diese Kopien, unabhängig vom verwendeten Medium, nach Bereinigung des Fehlers löschen. Wirkdaten dürfen nur zum Zweck der Fehleranalyse und ausschließlich auf dem bereitgestellten Equipment des Auftraggebers oder auf solchem des Auftragnehmers verwendet werden, sofern die vorherige Einwilligung des Auftraggebers vorliegt. Wirkdaten dürfen nicht ohne Zustimmung des Auftraggebers auf mobile Speichermedien (PDAs, USB- Speicher oder ähnliche Geräte) kopiert werden.

(9) Fernzugriffe im Rahmen von Prüfungs- und/oder Wartungsarbeiten sowie sämtliche in diesem Zusammenhang erforderlichen Tätigkeiten, insbesondere Tätigkeiten wie Löschen, Datentransfer oder eine Fehleranalyse, werden unter Berücksichtigung von technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten durchgeführt. In diesem Zusammenhang wird der Auftragnehmer die technischen und organisatorischen Maßnahmen wie im Anhang beschrieben ergreifen.

I. Anlage – Technisch-organisatorische Maßnahmen

#	Anforderung	Maßnahmen des Auftragnehmers
1	Pseudonymisierung (Art. 32 Abs. 1 litt. a DSGVO)	Ein Mandantentrennungskonzept regelt den Zugriff zu Systemen auf denen personenbezogene Daten verarbeitet werden. Zusätzlich werden für Testzwecke und Weiterentwicklungen ausschließlich pseudonymisierte Daten verwendet.
2	Verschlüsselung (Art. 32 Abs. 1 litt. a DSGVO)	Elektronische Kommunikationswege werden in geschlossenen Netzwerken abgesichert und zu übermittelnde Daten mit Hilfe von Kryptografischen Mittel verschlüsselt.
3	Sicherstellung Vertraulichkeit (Art. 32 Abs. 1 litt. b DSGVO)	- Zutrittskontrolle: A. Die Räumlichkeiten, in denen personenbezogene Daten erhoben, verarbeitet oder genutzt werden, werden ausschließlich von Mitarbeitern und zulässigerweise eingesetzten Dritten genutzt. Die Eingänge zu den Räumlichkeiten sind mit Sicherheits- oder digitalen Schlüsseln gegen Zutritt Unbefugter gesichert. Türen und Fenster sind außerhalb der Betriebszeiten fest verschlossen; Erdgeschossfenster zu den Räumlichkeiten verfügen über eine gesonderte Sicherung. Die Berechtigung zum Betreten der Räumlichkeiten wird durch geeignete Maßnahmen (Schlüssel-, Codeliste) zu dokumentiert. Die Vergabe dieser Berechtigung ist schriftlich protokolliert. Die Räumlichkeiten werden mit einer Alarmanlage mit Anschluss an eine Notrufzentrale und durch einen Sicherheitsdienst gesichert. - Zugangskontrolle: B. Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern. Die Server werden durch eine Firewall nach einem anerkannten Stand der Technik gegen Zugriffe von außen gesichert. Der Zugang ist nur befugten Mitarbeitern in dem zur Leistungserbringung erforderlichen Umfang gestattet und wird protokolliert. Die Protokolle werden stichpunktartig überprüft. - Zugriffskontrolle: C. Eingesetzte Systeme werden durch Benutzererkennung, Passwörter und abgestufte Zugriffsrechte geschützt. Die Zugriffsberechtigungen zu den eingesetzten Systemen werden nur an die zur Leistungserbringung eingesetzten Mitarbeiter in dem für die jeweilige Aufgabe erforderlichen Umfang vergeben, weiterhin Streng geheim gehalten und gegenüber unbefugten Dritten nicht bekannt zu machen. Bezüglich der technischen Wartung von Systemen werden gesonderte Zugriffsrechte vergeben, die möglichst keinen Zugriff auf personenbezogene Daten ermöglichen. Passwörter werden in ausreichender Komplexität gewählt (d.h. mindestens eine Länge von 8 (acht) Zeichen, keine Verwendung generischer Begriffe oder Eigennamen) sowie spätestens alle 2 Monate mittels automatisierter Abfrage geändert. - Weitergabekontrolle: D. Elektronische Kommunikationswege werden in geschlossenen Netzwerken abgesichert und zu übermittelnde Daten bei Bedarf mit Hilfe von Kryptografischen Mittel verschlüsselt. - Trennungskontrolle:

		E. Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden. Ein übergreifendes Berechtigungskonzept sowie Mandantentrennungskonzept regeln den Zugriff zu Systemen auf denen personenbezogene Daten verarbeitet werden.
4	Sicherstellung Integrität (Art. 32 Abs. 1 litt. b DSGVO)	- Eingabekontrolle: F. Jede Erstellung, Veränderung und Entfernung von Datensätzen unter gleichzeitiger Erfassung des Zeitpunktes und der eingebenden Person werden protokolliert.
5	Sicherstellung Verfügbarkeit (Art. 32 Abs. 1 litt. b DSGVO)	- Verfügbarkeitskontrolle: G. Es werden Vollwertige Sicherungskopien erstellt und an dafür vorgesehene Orte gelagert. Der Aufbewahrungsort schützt die Archivierungen vor Umwelteinflüssen und sonstigen Einflüssen durch Dritte. Die Tests der Datenwiederherstellung erfolgen regelmäßig.
6	Sicherstellung Belastbarkeit (Art. 32 Abs. 1 litt. b DSGVO)	Speicher-, Zugriffs- und Leitungskapazitäten werden den Anforderungen entsprechend regelmäßig geprüft und bewertet. Es erfolgen für System und Anwendungen regelmäßige Penetrationstest.
7	Gewährleistung zur raschen Wiederherstellung (Art. 32 Abs. 1 litt. c DSGVO)	Die Gewährleistung wird mittels Backupkonzepten, redundanter Datenhaltung hergestellt. Notfallkonzepte sowie Geschäftsfortführungspläne werden erstellt und regelmäßig überprüft und erprobt.
8	Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOMs (Art. 32 Abs. 1 litt. d DSGVO)	- Schutzbedarf feststellen, Risiken bewerten, geeignete Maßnahmen treffen (unter der Berücksichtigung von „Stand der Technik“, „Implementierungskosten“, Art, Umfang, Umstände und Zwecke der Verarbeitung“) und diese dokumentieren. - Betrieb eines Informationssicherheitsmanagementsystems, Incident-Response-Management und/oder eines Datenschutzmanagementsystems - Interne Prüfung: z.B. durch den Datenschutzbeauftragten, Informationssicherheitsbeauftragten, Revision sowie Business Continuity Manager - Externe Prüfung: durch z.B. Wirtschaftsprüfer: externe Revision sowie externe Prüfer für PS951 - Auftragskontrolle: Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.