Anlage Datenschutz

Datenschutz- und Datensicherheitsbestimmungen (DuD-B)

DZ BANK AG
Deutsche Zentral-Genossenschaftsbank,
Frankfurt am Main
Platz der Republik 60325 Frankfurt am Main

(nachstehend AUTRAGGEBER genannt)

und
…
…
…

(nachstehend AUFTRAGNEHMER genannt)

vereinbaren nachfolgende Anlage Datenschutz:

1. Die vorliegende Anlage „Datenschutz – und Datensicherheitsbestimmungen“ (DuD-B) konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus dem Vertrag ergeben. Sie findet Anwendung auf alle Leistungen oder Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Mitarbeiter des AUFTRAGNEHMERS oder durch den AUFTRAGNEHMER mit schriftlicher Zustimmung des AUFTRAGGEBERS beauftragte Subunternehmer personenbezogenen Daten des AUFTRAGGEBERS verarbeiten. Bezüglich des Abschluss dieser Anlage, Änderungen, Ergänzungen und Nebenabreden sowie der Zustimmung des AUFTRAGGEBERS zur Beauftragung von Subunternehmern kann – entgegen den Ausführungen in Teil 2, § 1 Abs. 15 – die Schriftform auch durch Verwendung eines von dem AUFTRAGGEBER angebotenen elektronischen Formats gemäß Art. 28 Abs.9 DS-GVO, z.B. eines elektronischen Bestellsystems, gewahrt werden.
2. Die Haftung der Parteien untereinander für Schäden im Zusammenhang mit der Auftragsverarbeitung richtet sich nach den Bestimmungen der DuD-B. Enthält die DuD-B keine diesbezüglichen Regelungen, gelten die gesetzlichen Bestimmungen (insbesondere Art. 82 Abs. 5 DS-GVO).
3. Die DuD-B finden weiterhin Anwendung bei Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen (Prüfung, Wartung und Pflege von Hard- oder Software), wenn dabei eine Verarbeitung, insbesondere der Zugriff auf personenbezogene Daten, nicht ausgeschlossen werden kann.
4. Ist der AUFTRAGGEBER ein Institut oder ist ein leistungsempfangendes Unternehmen innerhalb des Konzerns des AUFTRAGGEBERS ein Institut im Sinne des § 1 Abs. 1b Kreditwesengesetzes (KWG), gelten die Regelungen dieser Anlage entsprechend auch für alle sonstigen im Auftrag verarbeiteten Daten. Dies ist erforderlich, um einen gleichwertigen Schutz aller Daten zu erreichen, das Bankgeheimnis zu wahren und im Rahmen der besonderen organisatorischen Pflichten ein angemessenes und wirksames Risikomanagement im Sinne des § 25a KWG zu gewährleisten.

Die DuD-B bestehen aus:

Teil 1: Konkrete Angaben zur Auftragsverarbeitung

Teil 2: Allgemeine Regelungen zur Auftragsverarbeitung

Teil 3: Vereinbarung zur Festlegung der technischen und organisatorischen Maßnahmen

Teil 1

Konkrete Angaben zur Auftragsverarbeitung

Gemäß Art. 28 Abs. 3 Datenschutz–Grundverordnung (DS-GVO) sind folgende konkrete Angaben für den Auftrag festzulegen, sofern sie nicht bereits im Vertrag einschließlich seiner Anlagen geregelt wurden:

Zu löschender BEARBEITUNGSHINWEIS:

Zu löschende Ausfüllhilfe: Nachfolgende Ausführungen sind bei jedem Unternehmen der DZ BANK Gruppe individuell zu gestalten.

1. Gegenstand des Auftrages

Der AUFTRAGNEHMER verarbeitet personenbezogene Daten im Auftrag des AUFTRAGGEBERS.

☐

Der Gegenstand des Auftrags ergibt sich im Einzelnen aus dem Vertrag, auf den hier verwiesen wird. Soweit im Vertrag auf die Aufgaben des AUFTRAGNEHMERS Bezug genommen wird, sind die jeweiligen Vertragsvorschriften wesentlicher Bestandteil dieses Auftrages.

[Zu löschende Ausfüllhilfe: In der Leistungsbeschreibung muss der Auftrag zur Verarbeitung der personenbezogenen Daten mit einfachen sprachlichen Mitteln beschrieben sein , sodass nachvollziehbar wird, warum und für was der Auftragnehmer vom Auftraggeber eigentlich beauftragt wird. Die detaillierte Beschreibung der vom Auftragnehmer zu leistenden Aufgaben erfolgt dann in Ziffer 3b]

2. Dauer des Auftrages

☐ Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des Vertrags.

oder (insbesondere, falls im Vertrag keine Vorschrift zur Laufzeit besteht)

☐ Der Auftrag wird zur einmaligen Ausführung erteilt und endet, sobald die Leistung erbracht bzw. abgenommen ist.

oder

☐ Die Dauer dieses Auftrags (Laufzeit) ist befristet bis zum ***[Zu löschende Ausfüllhilfe: Fachbereich bitte Datum ergänzen].***

oder

☐ Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von ***[Zu löschende Ausfüllhilfe: Fachbereich Bitte Datum ergänzen]*** zum ***[Zu löschende Ausfüllhilfe: Fachbereich Bitte Datum ergänzen]*** gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

3. Art und Zweck der Verarbeitung von Daten

a) Zweck der Verarbeitung

☐ DV-Betrieb/Hosting der Applikation/der Anwendung (Rechenzentrum)	☐ Vernichtung von papierenen Datenträgern
☐ Drucken von Kontoauszügen	☐ Gehaltsabrechnung
☐ Markt- und Meinungsforschung	☐ Wertpapierabwicklung
☐ Telefonische Befragungen	☐ Daten-/ Anwendungsmigrationen
☐ Datenarchivierung	☐ Auswertungen
☐ Zahlungsverkehrsprozesse	☐
☐	☐

[Zu löschende Ausfüllhilfe: Die vorgenannten Aufzählungen sind beispielhaft und somit nicht abschließend. Sofern der Zweck einer Beauftragung hier nicht genannt ist, sind in den Leer-Feldern die erforderlichen Angaben nachvollziehbar aufzunehmen.

Zum Teil kann es hier – in Abhängigkeit von dem konkreten Vorhaben – zu einer Wiederholung der unter Ziffer 1 gemachten Angaben kommen. Eine solche etwaige Redundanz ist aber dem Gesetzestext geschuldet und daher hinzunehmen.]

b) Art der Verarbeitung (Beschreibung der einzelnen Verarbeitungsschritte)

Zur Erfüllung seiner Aufgaben und Erbringung seiner Leistungen gemäß vorliegendem Auftrag führt der AUFTRAGNEHMER die folgenden Arbeitsschritte durch:

[Zu löschende Ausfüllhilfe: Detaillierte Beschreibung der einzelnen Arbeitsschritte, bei denen personenbezogene Daten vom Auftragnehmer verarbeitet werden. Es ist davor zu warnen, hier zu allgemein zu formulieren. Ansonsten besteht die Gefahr, dass der Auftrag von bspw. der Datenschutzaufsichtsbehörde nicht als Auftragsverarbeitung eingestuft werden könnte.

Negativbeispiel: „Übernahme von Personalverwaltungsaufgaben".

Positivbeispiel: „Übernahme folgender Aufgaben aus der Personalverwaltung": (es haben hier dann zwingend detaillierte Darstellungen aller Tätigkeiten zu erfolgen, die übertragen werden, mit Angaben von Zeitpunkt und Umfang sowie des von den Arbeiten jeweils betroffenen Personenkreises (Verweis auf Ziffer 5)]

Beispiel einer detaillierten Beschreibung:

Der AUFTRAGNEHMER wird die vom AUFTRAGGEBER zur Verfügung gestellten Daten (vgl. nachfolgende Ziffer 4 „Art der Daten") in seinen Systemen speichern und damit auf

Grundlage des ihm zur Verfügung gestellten Mustertextes die Schreiben an die Beschäftigten (vgl. Ziffer 5 „Kreis der Betroffenen“) erstellen, diese jeweils auf dem ihm überlassenen Briefpapier ausdrucken und mit der entsprechenden Stellenbeschreibung zusammenfügen. Nach Fertigstellung der Schreiben wird der AUFTRAGNEHMER diese Schreiben dann an den AUFTRAGGEBER übergeben. Die Rückgabe des an den AUFTRAGNEHMER überlassenen USB-Sticks an den AUFTRAGGEBER erfolgt mit der Übergabe der erstellten Schreiben. Mit Beendigung des Auftrages wird der AUFTRAGNEHMER im Übrigen alle an ihn übergebenen Daten und Unterlagen datenschutzkonform vernichten bzw. löschen und dies dem AUFTRAGGEBER dann schriftlich unaufgefordert bestätigen.

4. Art der Daten

Im Zusammenhang mit der vorbeschriebenen Leistungserbringung werden vom AUFTRAGNEHMER folgende Datenarten/ -kategorien verarbeitet:

[Zu löschende Ausfüllhilfe: Detaillierte Beschreibung der personenbezogenen Datenarten/ -kategorien

Beispiele:

- ***Vorname;***
- ***Nachname;***
- ***Straße;***
- ***Postleitzahl;***
- ***Ort;***
- ***Anrede***
- ***Anredebezeichnung;***
- ***Geburtsdatum/Gründungdatum;***
- ***Personennummer;***
- ***Kundenberater;***
- ***Telefon privat;***
- ***Telefon geschäftlich;***
- ***Telefax.***

Es können aber auch nachvollziehbare Oberbegriffe gebildet und verwendet werden (bspw. Adressdaten usw.)]

5. Kategorien der betroffenen Personen

Die Kategorien der Personen, die durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags betroffen sind, umfassen:

[Zu löschende Ausfüllhilfe: Genaue Beschreibung der betroffenen Personenkreise

- Beispielsbeschreibungen:

-Kunden;
-Interessenten;
-Abonnenten;

-Beschäftigte i. S. d. § 26 Abs. 8 BDSG-neu;
-Lieferanten;
-Handelsvertreter;
-Ansprechpartner.]

6. Umfang der Weisungsbefugnisse, Verantwortliche Ansprechpartner bei den Parteien

Der AUFTRAGNEHMER darf während der Dauer des Auftrages die personenbezogenen Daten ausschließlich für die Zwecke gemäß Ziffer 1 entsprechend den unter Ziffer 3 Buchstabe b) dargestellten Verarbeitungsschritten verarbeiten, wenn und soweit dies mit den Bestimmungen zum Schutz personenbezogener Daten vereinbar ist. Darüber hinaus hat der AUFTRAGNEHMER alle weiteren konkreten und/oder generellen schriftlichen Weisungen des AUFTRAGGEBERS über Art, Umfang und Verfahren der Datenverarbeitung nach Maßgabe dieser DuD-B zu befolgen.

Weisungsberechtigte Personen des AUFTRAGGEBERS sind: *[Zu löschende Ausfüllhilfe: Bitte Name, Organisationseinheit, Funktion, Telefon ergänzen].*

Weisungsempfänger beim AUFTRAGNEHMER sind: *[Zu löschende Ausfüllhilfe: Auftragnehmer bitte Name, Organisationseinheit, Funktion, Telefon ergänzen].*

[Zu löschende Ausfüllhilfe:

- *Weisungsberechtigte Personen des Auftraggebers können solche Mitarbeiter des Auftraggebers sein, die im Zusammenhang mit einem Projekt / im Zusammenhang mit ihrem Aufgabenbereich, der ihnen jeweils innerhalb des Fachbereichs zugewiesen ist, hierfür zuständig sind und die berechtigterweise Zugriff auf die personenbezogenen Daten haben. Es können jeweils gleichzeitig auch mehrere Weisungsberechtigte Personen beim Auftraggeber benannt werden.*

- *Weisungsempfänger beim Auftragnehmer können solche Mitarbeiter des Auftragnehmers sein, die im Zusammenhang mit einem Projekt / im Zusammenhang mit ihrem Aufgabenbereich für die Auftragsabwicklung zuständig sind und die berechtigterweise Zugriff auf die personenbezogenen Daten haben. Es können jeweils gleichzeitig auch mehrere Weisungsempfänger beim Auftragnehmer benannt werden.]*

Betrieblicher Datenschutzbeauftragter des AUFTRAGGEBERS ist:

datenschutz@dzbank.de, Tel. 069/7447 94101 Feldf

Betrieblicher Datenschutzbeauftragter des AUFTRAGNEHMERS ist:

[Zu löschende Ausfüllhilfe: Bitte Kontaktdaten ergänzen].

Bei einem Wechsel oder einer längerfristigen Verhinderung des Ansprechpartners oder des Datenschutzbeauftragten ist dem Vertragspartner unverzüglich schriftlich der Nachfolger bzw. Vertreter mitzuteilen.

7. Etwaige Zustimmung zur Beauftragung von Subunternehmern

Gibt es nachfolgend keinen Eintrag unter Subunternehmer, ist dem AUFTRAGNEHMER die Beauftragung von einem oder mehreren Subunternehmern nicht gestattet.

Der AUFTRAGNEHMER darf folgenden/folgende Subunternehmer einsetzen:

-

-

Der/die vorgenannte/n Subunternehmer wird/werden mit folgenden Leistungen beauftragt:

-

-

8. Geltung der Anlage „Datenschutz- und Datensicherheitsbestimmungen“ (DuD-B)

Die DuD-B ist wesentlicher Bestandteil des Vertrages zwischen den Parteien.

Teil 2

Allgemeine Regelungen zur Auftragsverarbeitung

§ 1 Allgemeine Bestimmungen

1. Der AUFTRAGGEBER ist als „Verantwortlicher“ i.S.d. Art. 4 Nr. 7 Datenschutz-Grundverordnung (DS-GVO) für die Einhaltung der Vorschriften über den Datenschutz, für die Rechtmäßigkeit der Datenverarbeitung i.S.d. Art. 4 Nr. 2 DS-GVO, insbesondere der Datenweitergabe an den AUFTRAGNEHMER, sowie für die Wahrnehmung der Rechte der Betroffenen verantwortlich. Der AUFTRAGNEHMER hat den AUFTRAGGEBER hierbei in geeigneter Weise zu unterstützen. Darüber hinaus verpflichtet sich der AUFTRAGNEHMER zur Einhaltung sämtlicher einschlägiger datenschutzrechtlicher Vorschriften im Rahmen der Ausführung des Auftrages.
2. Sofern der AUFTRAGGEBER im Rahmen des jeweiligen Auftrages seinerseits selbst Dienstleister anderer Auftraggeber ist, stehen die Rechte aus dieser Anlage auch diesen anderen Auftraggebern zu.
3. Bei der E-Mail-Kommunikation werden die Parteien die Vertraulichkeit beachten, indem sie vertrauliche Informationen gegen unberechtigte Kenntnisnahme oder Manipulationen schützen. Hierzu können die Parteien entsprechende technische Maßnahmen, z.B. Verschlüsselungs- und Signaturverfahren, abstimmen.
4. Dem AUFTRAGNEHMER ist bekannt, dass ein Verstoß gegen datenschutzrechtliche Vorschriften eine Ordnungswidrigkeit und gegebenenfalls auch eine Straftatdarstellen kann.
5. Der AUFTRAGNEHMER bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind und dass der AUFTRAGGEBER und der AUFTRAGNEHMER und gegebenenfalls deren Vertreter bei Anfragen der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammenarbeiten.
6. Der AUFTRAGNEHMER bestätigt und stellt sicher, dass die für die Durchführung des Auftrags eingesetzten Personen zur Vertraulichkeit schriftlich verpflichtet sind und in die Schutzbestimmungen der DS-GVO eingewiesen worden sind. Die gleiche Verpflichtung gilt für weitere Bestimmungen zum Datenschutz (z.B. § 88 TKG sowie §§ 203, 206 StGB), sofern diese im konkreten Auftrag einschlägig sind. Auf Verlangen des AUFTRAGGEBERS wird der AUFTRAGNEHMER die Verpflichtung und Einweisung nachweisen.
7. Der AUFTRAGNEHEMER muss geeignete, wirksame und dokumentierte Maßnahmen implementieren, welche die Einhaltung der datenschutzrechtlichen Vorgaben sicherstellen, insbesondere im Hinblick auf das Erkennen und rechtzeitige Melden von Datenschutzverstößen.
8. Soweit der AUFTRAGNEHMER seine Leistung in den Räumlichkeiten oder unter Zugriff auf die Systeme des AUFTRAGGEBERS erbringt, unterliegt er den Kontrolleinrichtungen des AUFTRAGGEBERS (insbesondere Zutritts-, Zugangs- und Zugriffskontrolle).
9. Der AUFTRAGNEHMER ist für die Durchführung des Auftrages verpflichtet, nach Maßgabe der geltenden datenschutzrechtlichen Vorschriften einen Beauftragten für den Datenschutz schriftlich zu bestellen. Der AUFTRAGNEHMER wird dem AUFTRAGGEBER den Namen des Beauftragten für den Datenschutz benennen. Bei einem Wechsel des Beauftragten für den Datenschutz wird der AUFTRAGNEHMER den AUFTRAGGEBER unverzüglich hiervon in Kenntnis setzen. Soweit der AUFTRAGNEHMER nach Maßgabe der geltenden datenschutzrechtlichen Vorschriften nicht zur Bestellung eines Beauftragten für den Datenschutz verpflichtet ist, stellt er die Erfüllung der Aufgaben nach den geltenden datenschutzrechtlichen Vorschriften in anderer geeigneter Weise sicher.
10. 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.

11. Der AUFTRAGNEHMER unterstützt den AUFTRAGGEBER bei der Einhaltung der DS-GVO zur Sicherheit personenbezogener Daten, bei Meldepflichten bei Datenpannen, ggf. bei einer Datenschutz-Folgeabschätzungen und vorherige Konsultationen und insbesondere zur Erfüllung der Rechte der betroffenen Person gemäß Art.12 – 23 DS-GVO.
12. Datenschutzrechtliche Auskünfte an Dritte oder den Betroffenen darf der AUFTRAGNEHMER nur nach vorheriger schriftlicher Zustimmung durch den AUFTRAGGEBER erteilen.
13. Der AUFTRAGNEHMER und gegebenenfalls sein Vertreter und Subunternehmer führen ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DS-GVO zu allen Kategorien von im Auftrag des AUFTRAGGEBERS durchgeführten Tätigkeiten der Verarbeitung. Der AUFTRAGNEHMER wird dem AUFTRAGGEBER auf Anforderung die für diesen Vertrag relevanten Inhalte aus seinem Verarbeitungsverzeichnis zur Verfügung stellen.
14. Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB des AUFTRAGNEHMERS gegenüber dem AUFTRAGGEBER ist hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
15. Änderungen, Ergänzungen und Nebenabreden sowie einseitig abzugebende Willenserklärungen, wie z.B. Weisungen, Bestätigungen oder Zustimmungen, bedürfen der Schriftform gem. § 126 Bürgerliches Gesetzbuch (BGB). Dies gilt auch für Änderungen der Schriftformklausel.
16. Der AUFTRAGNEHMER verarbeitet personenbezogene Daten im Auftrag des AUFTRAGGEBERS. Dies umfasst Tätigkeiten, die im Hauptvertrag und in dieser Anlage konkretisiert sind.

§ 2 Ort der Datenverarbeitung

(1) Die Verarbeitung der Daten erfolgt ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR). Falls die Anwendung der DS-GVO in den Staaten des EWR nicht verbindlich beschlossen wurde, gelten die Staaten des EWR als Drittländer.

(2) Die Datenverarbeitung in Drittländern ist unzulässig. Dies gilt auch für Subunternehmer, wobei darauf hingewiesen wird, dass unter „Verarbeitung“ auch die Möglichkeit der Einsichtnahme, etwa im Rahmen von Fernwartungszugriffen zu verstehen ist.

(3) Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des AUFTRAGGEBERS und kann nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

(4) Die Verarbeitung von Daten außerhalb von Betriebsstätten des AUFTRAGNEHMERS (z.B. Heim-/Telearbeit, Remotezugriff) ist unzulässig.

§ 3 Weisungsrecht und Zweckbindung

(1) Bei der Verarbeitung personenbezogener Daten wird der AUFTRAGNEHMER für den AUFTRAGGEBER tätig und ist insoweit verpflichtet, die Daten ausschließlich zur Erbringung der vertraglich vereinbarten Leistungen und für Zwecke des AUFTRAGGEBERS zu verarbeiten und dabei den schriftlichen Weisungen des AUFTRAGGEBERS zu folgen.

(2) Kopien oder Duplikate 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) Mündliche Weisungen sind unverzüglich schriftlich durch den AUFTRAGNEHMER zu bestätigen. Die schriftliche Bestätigung der mündlichen Weisungen muss von AUFTRAGGEBER und AUFTRAGNEHMER so aufbewahrt werden, dass alle maßgeblichen Regelungen jederzeit verfügbar sind.

(4) Der AUFTRAGNEHMER hat den AUFTRAGGEBER unverzüglich darauf aufmerksam zu machen, wenn eine vom AUFTRAGGEBER erteilte Weisung seiner Meinung nach gegen Vorschriften über den Datenschutz verstößt.

§ 4 Unverzüglich Meldungen und Informationspflichten bei Datenschutzverletzungen

(1) Der AUFTRAGNEHMER hat den AUFTRAGGEBER bei Unregelmäßigkeiten des Datenverarbeitungsablaufes, bei begründetem Verdacht der Verletzung von Vorschriften und vertraglichen Vereinbarungen zum Schutz personenbezogener Daten, Verstöße des AUFTRAGNEHMERS oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen, sowie bei Beanstandungen durch eine Datenschutzaufsichtsbehörde, eine Revision oder in sonstigen Datenschutzprüfungsberichten, sofern ihm dies nicht aufgrund einer behördlichen Vorgabe im Rahmen eines Ermittlungsverfahrens untersagt ist, zu informieren und die Abhilfemaßnahmen aufzuzeigen (Datenschutzverletzung). Der AUFTRAGNEHMER sichert zu, den AUFTRAGGEBER bei möglichen Informationspflichten nach Artikel 33 – 34 DS-GVO zu unterstützen.

(2) Die Meldung an den AUFTRAGGEBER muss unverzüglich und möglichst binnen 24 Stunden, nachdem dem AUFTRAGNEHMER die Verletzung bekannt wurde erfolgen.

(3) Jede Datenschutzverletzung ist vom AUFTRAGNEHMER zu dokumentieren. Die Dokumentation und Meldung einer Datenschutzverletzung enthält mindestens folgende Informationen:

1. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
2. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
3. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
4. eine Beschreibung der von dem AUFTRAGNEHMER ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Darüber hinaus hat der AUFTRAGNEHMER dem AUFTRAGGEBER alle sonstigen Informationen zu erteilen, die der AUFTRAGGEBER für die Erfüllung seiner eigenen Meldepflichten benötigt.

(4) Sofern die Möglichkeit besteht, dass das Eigentum des AUFTRAGGEBERS an den Daten beim AUFTRAGNEHMER durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet wird oder absehbar gefährdet werden könnte, so hat der AUFTRAGNEHMER den AUFTRAGGEBER unverzüglich zu verständigen.

(5) Der AUFTRAGNEHMER hat dem AUFTRAGGEBER alle aus einer Datenschutzverletzung entstehenden Schäden, insbesondere die Kosten für die Benachrichtigung der Betroffenen oder ein etwaiges Bußgeld bei Verletzung der Selbstanzeigepflicht nach Artikel 33 – 34 DS-GVO zu ersetzen, sofern dem ein schuldhaftes Verhalten des AUFTRAGNEHMERS zugrunde liegt.

§ 5 Subunternehmer

(1) Der Einsatz von Subunternehmern durch den AUFTRAGNEHMER und/oder weiterer Subunternehmer (Kettenbeauftragung) bedarf der vorherigen schriftlich Zustimmung des AUFTRAGGEBERS.

(2) Der AUFTRAGGEBER behält sich vor, die Zustimmung lediglich zu erteilen, nachdem der AUFTRAGNEHMER Namen und Anschrift des Subunternehmers mitgeteilt hat. Ferner behält sich der AUFTRAGGEBER vor, die Zustimmung lediglich zu erteilen, sofern vom AUFTRAGNEHMER nachgewiesen wurde, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt hat.

(3) Der AUFTRAGNEHMER hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen AUFTRAGGEBER und AUFTRAGNEHMER auch gegenüber Subunternehmern gelten. Insbesondere muss der AUFTRAGGEBER berechtigt sein, Kontrollen vor Ort beim Subunternehmer durchzuführen oder durch Dritte durchführen zu lassen. Der AUFTRAGNEHMER hat die Einhaltung der Pflichten regelmäßig zu überprüfen.

(4) Die schriftlich zu treffenden, vertraglichen Vereinbarungen zwischen dem AUFTRAGNEHMER und dem Subunternehmer sind so zu gestalten, dass sie den Regelungen der vorliegenden Anlage entsprechen. Zu diesem Zweck müssen insbesondere die mit dem Subunternehmer zu vereinbarenden technischen und organisatorischen Maßnahmen ein gleichwertiges Schutzniveau aufweisen; die Weisungs- und Kontrollrechte müssen uneingeschränkt erhalten bleiben und die Datenverarbeitung muss weiterhin in der EU/EWR erfolgen.

(5) Auf Anforderung des AUFTRAGGEBERS wird der AUFTRAGNEHMER Auskunft über den wesentlichen Vertragsinhalt mit dem Subunternehmer und die Umsetzung der datenschutzrelevanten Verpflichtungen geben, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen.

(6) Bedient sich der AUFTRAGNEHMER bei der Erbringung der Leistung gegenüber dem AUFTRAGGEBER eines Subunternehmers, wird der AUFTRAGNEHMER dem AUFTRAGGEBER unverzüglich auf Verlangen die Dokumentation und das Ergebnis der vom AUFTRAGNEHMER in Bezug auf den Subunternehmer durchgeführten Erstkontrolle und regelmäßigen Kontrollen bzw. die Einhaltungsbestätigungen des Subunternehmers zugänglich machen.

(7) Der AUFTRAGNEHMER bleibt für die Erfüllung der auf den Subunternehmer übertragenen Tätigkeiten im gleichen Umfang verantwortlich, als würden diese durch den AUFTRAGNEHMER selbst ausgeführt. Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters.

§ 6 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) Der AUFTRAGGEBER kann vorbehaltlich gesetzlicher Aufbewahrungspflichten oder sonstiger entgegenstehender Rechtsvorschriften auch während der Laufzeit und nach Beendigung des Vertrages jederzeit die Berichtigung, Löschung, Sperrung (i.S.d. Einschränkung der Verarbeitung gem. Art. 4 Nr. 3 DS-GVO) und Herausgabe von personenbezogenen Daten verlangen.

(3) Nach Abschluss der vertraglichen Arbeiten hat der AUFTRAGNEHMER, sämtliche in seinen Besitz gelangten Unterlagen, wie z.B. Test- und Ausschussmaterial, Datensicherungsko-

pien und erstellten Verarbeitungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, datenschutzkonform zu löschen oder dem AUFTRAGGEBER auszuhändigen. Dokumente, Daten und Kopien die nicht ausgehändigt werden können sind nach Abschluss der vertraglichen Arbeiten zu löschen. Die Löschung ist durch ein entsprechendes Löschprotokoll nachzuweisen. Gesetzliche Aufbewahrungspflichten, denen der AUFTRAGNEHMER unterliegt insbesondere nach Abgabenordnung und HGB, bleiben hiervon unberührt. Vertragsbezogene Daten (z.B. Ansprechpartner des AUFTRAGGEBERS), die zur Sicherung von Beweisinteressen des AUFTRAGNEHMERS erforderlich sind, dürfen in gesperrter Form bis zum Ablauf der hierfür geltenden Verjährungsfrist aufbewahrt werden. Die Löschung ist dem AUFTRAGGEBER auf Anforderung schriftlich zu bestätigen. Zurückbehaltungsrechte des AUFTRAGNEHMERS sind ausgeschlossen.

(4) Soweit eine betroffene Person sich diesbezüglich unmittelbar an den AUFTRAGNEHMER wendet, wird der AUFTRAGNEHMER dieses Ersuchen unverzüglich an den AUFTRAGGEBER weiterleiten.

§ 7 Technische und organisatorische Sicherheitsmaßnahmen nach Art.32 DS-GVO

(1) Der AUFTRAGNEHMER wird seine Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind.

(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.

(3) Der AUFTRAGNEHMER beachtet die Grundsätze für die Verarbeitung personenbezogener Daten aus Art. 5 Abs. 1, Abs. 2 DS-GVO und gewährleistet die vertraglich vereinbarten und gesetzlich erforderlichen Datensicherheitsmaßnahmen gem. Art. 24, Art. 28, Art. 32 DS-GVO, um den Nachweis zu erbringen, dass die Verarbeitung gemäß der DS-GVO erfolgt.

(4) Der AUFTRAGNEHMER darf Zugriffsberechtigungen nur an Personen vergeben, die mit der Durchführung des Auftrags befasst sind. Die Berechtigungen sind nur in dem für die Erfüllung der jeweiligen Aufgaben erforderlichen Umfang zu vergeben. Auf Verlangen wird der AUFTRAGNEHMER dem AUFTRAGGEBER die zugriffsberechtigten Personen und deren Berechtigungen benennen.

(5) Der AUFTRAGNEHMER sichert zu, dass die verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

(6) Der AUFTRAGNEHMER ist nicht befugt, ohne schriftliche Einwilligung des AUFTRAGGEBERS Hard- oder Software an die Systeme des AUFTRAGGEBERS anzuschließen oder darauf zu installieren.

(7) Dem AUFTRAGNEHMER ist es nicht gestattet, personenbezogene Daten in Systeme Dritter einzuspielen. Dies gilt auch für Testzwecke.

(8) Dem AUFTRAGNEHMER ist es nicht gestattet während der Entwicklung von Software oder der Prüfung und Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen des AUFTRAGGEBERS personenbezogenen Daten des AUFTRAGGEBERS zu verwenden. Hierfür sind fiktive Testdaten oder nach ausdrücklicher schriftlicher Einwilligung durch den AUFTRAGGEBER anonymisierte Originaldaten zu verwenden.

(9) Zum Schutz personenbezogener Daten vor Missbrauch und Verlust (Datensicherheit) wird der AUFTRAGNEHMER die technischen und organisatorischen Maßnahmen treffen, auf die sich die Parteien entsprechend in Teil 3 der DuD-B TOM, verständigt haben.

(10) Die vereinbarten Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung und sind vom AUFTRAGNEHMER dem aktuellen Stand der Technik anzupassen.

Dies gilt ebenso im Fall von Anordnungen der zuständigen Aufsichtsbehörden. Beabsichtigte wesentliche Änderungen (z.B. wesentliche Änderung von Verschlüsselungsverfahren oder Anmeldeprozeduren) sind zu dokumentieren und dem AUFTRAGGEBER mitzuteilen sowie einvernehmlich in einer geänderten Fassung des Teil 3 der DuD-B, der „Vereinbarung zur Festlegung der technischen und organisatorischen Maßnahmen“ festzuhalten, wobei der AUFTRAGGEBER Änderungen nicht ohne erheblichen Grund widerspricht.

§ 8 Ermöglichung von Kontrollen und Zurverfügungstellung von Informationen

(1) Der AUFTRAGNEHMER erklärt sich damit einverstanden, dass der AUFTRAGGEBER jederzeit berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang selbst oder durch Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort. Der AUFTRAGNEHMER sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen mitwirkt. Entstehende Kosten bei der Durchführung der Kontrollen werden nicht erstattet.

(2) Der AUFTRAGNEHMER gewährleistet die ordnungsgemäße Durchführung der technischen und organisatorischen Maßnahmen (Teil 3 der DuD-B, „TOM“). Die Einhaltung der technischen und organisatorischen Maßnahmen wird der AUFTRAGNEHMER regelmäßig durch geeignete Nachweise z.B. von seiner Revision, seinem betrieblichen Datenschutzbeauftragten oder einer anerkannten Wirtschaftsprüfungsgesellschaft, belegen (Einhaltungsbestätigung).

(3) Die Einhaltungsbestätigung ist vom AUFTRAGNEHMER dem AUFTRAGGEBER vor Beginn der Datenverarbeitung und danach sofern im Einzelfall nichts Anderes vereinbart wird, unaufgefordert jährlich vorzulegen bzw. bereitzustellen. Unabhängig davon räumt der AUFTRAGNEHMER dem AUFTRAGGEBER und dessen Bevollmächtigten bezüglich der vereinbarten technischen und organisatorischen Maßnahmen ein Besichtigungs-, Einsichtnahme-, Auskunfts- und Kontrollrecht (Prüfungsrechte), grundsätzlich nach vorheriger Abstimmung mit dem AUFTRAGNEHMER und während dessen gewöhnlichen Geschäftszeiten, ein. Der AUFTRAGNEHMER ist verpflichtet, im Falle von Auskünften und Einsichtnahmen die erforderliche Unterstützung bereitzustellen. Im Übrigen wird der AUFTRAGNEHMER den Personen, die Prüfungen oder sonstige Maßnahmen vornehmen, den Zugang zu allen Räumlichkeiten und Liegenschaften zwecks Einhaltung der gesetzlichen Prüfpflichten des AUFTRAGGEBERS gewähren.

Teil 3

Vereinbarung zur Festlegung der technischen und organisatorischen Maßnahmen (TOM)

Vereinbarung zur Festlegung der technischen und organisatorischen Maßnahmen

Der AUFTRAGNEHMER trifft geeignete technische und organisatorische Maßnahmen (Art. 32 DS-GVO), um ein dem Risiko angemessenes Schutzniveau im Hinblick auf die erforderliche Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer zu gewährleisten.

[Bitte beachten Sie hierzu die beigefügten Ausfüllhinweise sowie die Anweisung zur Erstellung des Nachweises zur Einhaltung der vereinbarten technischen und organisatorischen Maßnahmen.

Diese Maßnahmen schließen folgendes ein:

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

- **Zutrittskontrolle**

  Maßnahmen die Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden verwehren:
  [Zu löschender BEARBEITUNGSHINWEIS: IST VOM AUFTRAGNEHMER AUSZUFÜLLEN UND DEM AUFTRAGGEBER NACHZUWEISEN]

- **Zugangskontrolle**

  Maßnahmen die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:
  [Zu löschender BEARBEITUNGSHINWEIS: IST VOM AUFTRAGNEHMER AUSZUFÜLLEN UND DEM AUFTRAGGEBER NACHZUWEISEN]

- **Zugriffskontrolle**

  Maßnahmen die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

  [Zu löschender BEARBEITUNGSHINWEIS: IST VOM AUFTRAGNEHMER AUSZUFÜLLEN UND DEM AUFTRAGGEBER NACHZUWEISEN]

- **Trennungskontrolle**

  Maßnahmen die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:
  [Zu löschender BEARBEITUNGSHINWEIS: IST VOM AUFTRAGNEHMER AUSZUFÜLLEN UND DEM AUFTRAGGEBER NACHZUWEISEN]

- **Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)**

  Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen:
  [Zu löschender BEARBEITUNGSHINWEIS: IST VOM AUFTRAGNEHMER NUR AUSZUFÜLLEN UND DEM AUFTRAGGEBER NACHZUWEISEN, WENN MIT DEM AUFTRAGGEBER VEREINBART, TRIFFT NUR IN AUSNAHMEFÄLLEN ZU]

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

- **Weitergabekontrolle**

  Maßnahmen die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:
  [Zu löschender BEARBEITUNGSHINWEIS: IST VOM AUFTRAGNEHMER AUSZUFÜLLEN UND DEM AUFTRAGGEBER NACHZUWEISEN]

- **Eingabekontrolle**

  Maßnahmen die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:
  [Zu löschender BEARBEITUNGSHINWEIS: IST VOM AUFTRAGNEHMER AUSZUFÜLLEN UND DEM AUFTRAGGEBER NACHZUWEISEN]

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

- **Verfügbarkeitskontrolle und rasche Wiederherstellbarkeit**

  Maßnahmen die gewährleisten, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind:
  [Zu löschender BEARBEITUNGSHINWEIS: IST VOM AUFTRAGNEHMER AUSZUFÜLLEN UND DEM AUFTRAGGEBER NACHZUWEISEN]

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

- **Datenschutz-Management**

[Zu löschender BEARBEITUNGSHINWEIS: IST VOM AUFTRAGNEHMER AUSZUFÜLLEN UND DEM AUFTRAGGEBER NACHZUWEISEN]

- **Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)**
  - Löschungen in den für die Verarbeitung eingesetzten Systemen können durchgeführt werden (Löschfähigkeit).
  - Es werden nur die gemäß Vorgaben des Auftraggebers erforderlichen Daten verarbeitet

[Zu löschender BEARBEITUNGSHINWEIS: DIESE BEIDEN PUNKTE SIND VOM AUFTRAGNEHMER ZU BESTÄTIGEN, GGF. UM VORHANDENE WEITERE MASSNAHMEN ZU ERGÄNZEN SOWIE DEM AUFTRAGGEBER NACHZUWEISEN]

- **Auftragskontrolle**

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

[Zu löschender BEARBEITUNGSHINWEIS: IST VOM AUFTRAGNEHMER AUSZUFÜLLEN UND DEM AUFTRAGGEBER NACHZUWEISEN]

Ausfüllhinweise

zur Vereinbarung zu den technischen und organisatorischen Maßnahmen

AUSFÜLLHINWEISE FÜR AUFTRAGNEHMER -- SEITE VOR VERTRAGSUNTERZEICHNUNG ENTFERNEN !!!

Bitte geben Sie an, welche konkreten technischen und organisatorischen Maßnahmen Sie zur Gewährleistung von Datenschutz und Datensicherheit getroffen haben und liefern Sie uns hierzu einen Nachweis.

Eine Maßnahme zur Gewährleistung von Vertraulichkeit und Integrität ist insbesondere die Verwendung von dem Stand der Technik entsprechenden ***Verschlüsselungsverfahren****. Im Übrigen sind Beispielmaßnahmen nachfolgend aufgeführt.*

Die einzelnen Maßnahmen sind nachvollziehbar zu erläutern.

Die Vereinbarung zu den technischen und organisatorischen Maßnahmen ist Bestandteil der ***Anlage*** *Datenschutz (DuD-B).*

Beispielmaßnahmen zur Vertraulichkeit (Nr. 1):

Zutrittskontrolle

- Kartengestützte personalisierte Zutrittskontrollsysteme mit Zutrittsberechtigung nur für autorisierte Mitarbeiter,
- Dienstanweisungen zur Handhabung von Zutrittskontrollen,
- Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
- Mit Zahlenschloss gesicherte Serverräume (Code ist nur Mitarbeitern der IT-Abteilung bekannt und wird regelmäßig geändert),
- Vergaberichtlinien für Zutrittsberechtigungen zu den Serverräumen,
- Server in abschließbaren Serverschränken, Schlüssel bei IT-Abteilung,
- Organisationsanweisung zur Ausgabe von Schlüsseln,
- Aufbewahrung von Sicherungsbändern in zugriffsgeschütztem Safe,
- Verschluss von Laptops in Schränken nach Dienstschluss,
- Abschließen des Gebäudes nach Arbeitsschluss sowie Sicherung durch Alarmanlage und Wachdienst mit regelmäßigen Kontrollgängen,
- Vergitterte Fenster

Zugangskontrolle

- Serversysteme nur mit Konsolenpasswort oder über passwortgeschützte, verschlüsselte Verbindung administrierbar
- Datenverschlüsselung
- Clientsysteme nur nach passwortgestützter Netzwerk-Authentifizierung nutzbar
- Sperrung des Benutzerkontos nach drei fehlgeschlagenen Anmeldeversuchen
- Automatische, passwortgeschützte Bildschirm- und Rechnersperre nach 10 Minuten
- Revisionssicheres, verbindliches Verfahren zur Rücksetzung „vergessener“ Passwörter
- Revisionssicheres, verbindliches Verfahren zur Vergabe von Berechtigungen
- Eindeutige Zuordnung von Benutzerkonten zu Benutzern, keine unpersönlichen Sammelkonten („AZUBI1“)
- Richtlinie zum sicheren, ordnungsgemäßen Umgang mit Passworten/Smartcards
- Automatisierte Standardroutinen für regelmäßige Aktualisierung von Schutzsoftware (z.B. Virenscanner)

AUSFÜLLHINWEISE FÜR AUFTRAGNEHMER -- SEITE VOR VERTRAGSUNTERZEICHNUNG ENTFERNEN !!!

Zugriffskontrolle

- Datenverschlüsselung
- Berechtigungsmechanismus mit Möglichkeit zur exakten Differenzierung auf Feldebene
- Revisionssicheres, verbindliches Berechtigungsvergabeverfahren
- Revisionssicheres, verbindliches Verfahren zur Wiederherstellung von Daten aus Backup (Restore durch IT-Abteilung auf Anweisung von Projektleitung / Abteilungsleitung / Geschäftsleitung / Geschäftsführung)
- Trennung von Berechtigungsbewilligung (organisatorisch) durch Abteilungsleitung / Geschäftsleitung / Geschäftsführung und Berechtigungsvergabe (technisch) durch IT-Abteilung
- Netzlaufwerke mit Zugriff nur für berechtigte Benutzer(gruppen)

Trennungskontrolle

- Die Daten des Auftraggebers und anderer Mandanten werden soweit möglich von unterschiedlichen Mitarbeitern des Auftragnehmers verarbeitet
- Es existiert ein Berechtigungskonzept, das der getrennten Verarbeitung von Daten des Auftraggebers von Daten anderer Mandanten Rechnung trägt
- Die in den verwendeten Systemen verfügbaren Berechtigungsmechanismen ermöglichen die exakte Umsetzung der Vorgaben des Berechtigungskonzeptes

Pseudonymisierung

- Maßnahmen zur Pseudonymisierung werden nur in Ausnahmefällen möglich und mit dem Auftraggeber vereinbart sein (z.B. für Testdurchführungen)

Beispielmaßnahmen zur Integrität (Nr. 2):

Weitergabekontrolle

- Transport von Sicherungsbändern in Sicherungssafe per hauseigenem Kurier
- Versand personenbezogener Daten, z.B. per verschlüsselter E-Mail
- Datenverschlüsselung
- Leitungsverschlüsselung

Eingabekontrolle

- Vertragliche Beschränkung der Arbeit mit personenbezogenen Daten des Auftraggebers auf die im Zusammenhang mit Leistungen aus dem Vertrag tätigen Mitarbeiter des Auftragnehmers
- Registrierung der Benutzer und Uhrzeit der jeweiligen Änderung im Teilnehmerverwaltungssystem

Beispielmaßnahmen zur Verfügbarkeit und Belastbarkeit (Nr. 3):

- Vollständiges Backup- und Recovery-Konzept mit täglicher Sicherung und katastrophensicherer Aufbewahrung der Datenträger
- Nachweis der sicheren und ordnungsgemäßen Archivierung in physisch geschütztem Archiv und verbindlicher Regelung der Zugriffsberechtigten
- Sachkundiger Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter) und schriftliche Konzeption ihres Einsatzes (Virenschutzkonzept usw.)
- Einsatz von Festplattenspiegelung
- Einsatz unterbrechungsfreier Stromversorgung

Beispielmaßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Nr. 4):

Datenschutzmanagement

- Der Auftragnehmer hat einen betrieblichen Datenschutzbeauftragten bestellt und sorgt durch die Datenschutzorganisation für dessen angemessene und effektive Einbindung in die relevanten betrieblichen Prozesse
- Regelmäßige Audits (extern)
- Regelmäßige Prüfungen der Innenrevision

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

- Die angegebenen Aspekte zur Löschung und Datenspeicherung sind gesetzlich vorgeschrieben und die erwarteten Mindestanforderungen an dieser Stelle.
- Weitere vorhandene Vorkehrungen des Auftragnehmers sollen auch angegeben werden.

Auftragskontrolle

- Der Vertrag enthält detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers
- Der Vertrag enthält detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des Auftraggebers sowie ein Verbot der Nutzung durch den Auftragnehmer außerhalb des schriftlich formulierten Auftrags
- Auf Wunsch des Auftraggebers kann im Vertrag eine verantwortliche Person beim Auftragnehmer benannt werden, die in Bezug auf die vereinbarte Auftragsdatenverarbeitung gegenüber dem Auftragnehmer weisungsbefugt ist

Anweisung zur Erstellung eines Nachweises betreffend die Einhaltung der vereinbarten technischen und organisatorischen Maßnahmen

AUSFÜLLHINWEISE FÜR AUFTRAGNEHMER – SEITE VOR VERTRAGSUNTERZEICHNUNG ENTFERNEN !!!

Gemäß Art. 28 DS-GVO hat sich der Auftraggeber von der Einhaltung der beim Auftragnehmer getroffenen und in der Anlage Datenschutz (DuD-B) des Vertrages vereinbarten technischen und organisatorischen Maßnahmen (TOM) regelmäßig zu überzeugen. Anstelle einer beim Auftragnehmer durchzuführenden Vor-Ort-Überprüfung sieht es der Auftraggeber gegenwärtig grundsätzlich als ausreichend an, sich mittels eines Nachweises von der Einhaltung der vereinbarten Maßnahmen im Hause des Auftragnehmers zu überzeugen.

Der Auftragnehmer ist deshalb gehalten, dem Auftraggeber einen entsprechenden Nachweis zukommen zu lassen, aus dem hervorgeht, dass die zwischen ihm und dem Auftragnehmer vereinbarten und im Hause des Auftragnehmers getroffenen technischen und organisatorischen Maßnahmen eingehalten werden. Den Nachweis kann der Auftragnehmer durch die Vorlage eines aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, seiner Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erbringen.

In diesem Zusammenhang ist dem Auftraggeber zu bestätigen, dass die innerbetriebliche Organisation des Auftragnehmers so gestaltet ist, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Des Weiteren sind werthaltige Aussagen im Hinblick auf die erforderlichen Datenschutz- und -sicherheitsmaßnahmen (Art. 32 DS-GVO) zu treffen.

Ferner hat der Auftragnehmer dem Auftraggeber zu bestätigen, dass

- die ihm überlassenen Daten ausschließlich zur Erbringung der vertraglich vereinbarten Leistungen und gemäß den Weisungen des Auftraggebers verarbeitet werden,
- beim Umgang mit den überlassenen Daten nur Personal eingesetzt wird, das auf einen datenschutzkonformen Umgang mit personenbezogenen Daten (insbesondere die Geheimhaltung der Daten) gemäß der DS-GVO sowie weiterer maßgeblicher Bestimmungen zum Datenschutz eingewiesen und verpflichtet worden ist,
- nur Unterauftragnehmer eingesetzt werden, die der Auftragnehmer hinsichtlich deren getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt und sich vor Beginn der Datenverarbeitung und sodann jährlich (sofern im Einzelfall nichts Anderes vereinbart wurde) bezüglich der Einhaltung überzeugt hat,
- dem Auftragnehmer für die Beauftragung dieser Unterauftragnehmer jeweils die Einwilligung des Auftraggebers vorliegt,
- die zwischen den Auftragnehmer und Unterauftragnehmern (Kettenbeauftragung) vertraglich getroffenen Vereinbarungen so gestaltet sind, dass sie den vertraglich festgelegten Regelungen (Datenschutz- und Datensicherheitsbestimmungen – DuD-B) zwischen dem Auftraggeber und dem Auftragnehmer entsprechen. Dies betrifft insbesondere die technischen und organisatorischen Maßnahmen, welche ein gleichwertiges Schutzniveau aufweisen müssen,
- der Auftragnehmer im Zusammenhang mit der vertraglich vereinbarten Leistungserbringung keine Unterauftragnehmer einsetzt, deren Betriebsstätte sich außerhalb der EU/EWR[1]-Staaten (Drittland) befindet bzw. die von einem Drittland Zugriff auf die überlassenen Daten haben. Hierzu zählen auch die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen, wenn dabei ein Zugriff auf die überlassenen Daten nicht ausgeschlossen werden kann und
- die beim Auftragnehmer für die Erbringung der vereinbarten Leistungen eingesetzten Verfahren einem regelmäßigen Audit resp. Kontrolle unterliegen.

[1] Sofern die Anwendung der DS-GVO in den Staaten des EWR verbindlich beschlossen wurde.

Aus der vorgenannten Bestätigung muss schließlich ersichtlich sein:

- wer im Hause des Auftragnehmers die Audits bzw. Kontrollen durchgeführt hat,
- wann und mit welchen Schwerpunkten die letzten Kontrollen durchgeführt wurden,
- wie das Prüfungsergebnis lautet (welche Beanstandungen; werden/wurden Feststellungen zeitnah behoben etc.),
- und in welchem Zeitintervall die vereinbarten technischen und organisatorischen Maßnahmen geprüft werden.

Der Auftragnehmer hat, sofern noch nicht geschehen, dem Auftraggeber den derzeitigen Datenschutzbeauftragten in seinem Hause mit Kontaktdaten bekannt zu geben.

Der Auftragnehmer hat einen Nachweis im vorbeschriebenen Umfang dem Auftragnehmer unaufgefordert vorzulegen:

- vor Beginn der Leistungserbringung (Datenverarbeitung) und danach
- regelmäßig einmal jährlich (gerechnet ab dem Zeitpunkt der erstmaligen Leistungserbringung) sofern im Einzelfall nichts Anderes vereinbart wurde

AUSFÜLLHINWEISE FÜR AUFTRAGNEHMER -- SEITE VOR VERTRAGSUNTERZEICHNUNG ENTFERNEN !!!