Datenschutz

Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO

VERANTWORTLICHER, NACHFOLGEND AUFTRAGGEBER (AG) GENANNT:

Degewo AG
Potsdamer Straße 60
10785 Berlin

AUFTRAGSVERARBEITER, NACHFOLGEND AUFTRAGNEHMER (AN) GENANNT:

Name:
Straße:
Ort

PRÄAMBEL

Der AN führt im Auftrag des AG Tätigkeiten aus, welche weisungsgebundene Verarbeitungen von personenbezogenen Daten beinhalten. Dies stellt eine Auftragsverarbeitung im Sinne des Art. 28 EU Datenschutz-Grundverordnung (DSGVO) dar. Dieser liegen die Regelungen der DSGVO und des Bundesdatenschutzgesetzes (BDSG) zugrunde. Der vorliegende Vertrag zur Auftragsverarbeitung stellt die vertragliche Regelung der ordnungsgemäßen Verarbeitung personenbezogener Daten durch den AN im Auftrag des AG dar. Der Verantwortliche für die Verarbeitung im Sinne des Art. 4 Nr. 7 sowie Art. 28 DSGVO ist der AG. Die Anlage 1 „Weitere Auftragsverarbeiter“ und Anlage 2 „Technische und organisatorische Maßnahmen“ sind Bestandteil dieses Vertrags zur Auftragsverarbeitung.

§ 1 GRUNDLAGE, GEGENSTAND, DAUER UND KÜNDIGUNG DES VERTRAGS

1. Die Grundlage dieses Auftrags ist: Durchführung der Mieterratswahl 2027

2. Kurzbeschreibung der Leistung: Erstellung von Agentur-, Grafik-, Druck- und Lettershop-Dienstleistungen für die Durchführung der Mieterratswahl

3. Laufzeit des Vertrags: 01.12.2026 – 30.11.2027

4. Kündigung des Vertrags: entfällt

§ 2 ART UND ZWECK DER VERARBEITUNG DER DATEN

1. Die Art und der Zweck der Verarbeitung der personenbezogenen Daten:

2. Zu dem genannten Zweck dürfen Daten nur auf:

☐ den IT-Systemen des AG

☐ den IT-Systemen der AN inkl. Subunternehmen

☐ den IT-Systemen des AG und AN inkl. Subunternehmen

verarbeitet werden.

Hinweis: Bitte die zutreffenden Fälle ankreuzen.

§ 3 ART DER PERSONENBEZOGENEN DATEN UND DIE KATEGORIEN BETROFFENER PERSONEN:

1. Die Arten der von der Verarbeitung erfassten Daten sind:

2. Die Kategorien betroffener Personen der Datenverarbeitung sind:

☐ Kunden

☐ Mietende

☐ Beschäftigte

☐ Ansprechpartner von Lieferanten/ Dienstleistern

☐ Weitere:

Hinweis: Bitte die zutreffenden Fälle ankreuzen.

§ 4 ZWECKBINDUNG UND WEISUNGSBEFUGNIS DES AG

1. Die Daten des AG sind von den Daten anderer AG und denen des AN getrennt zu verarbeiten. Ferner ist es dem AN untersagt, die Daten des AG für andere als für die vertragsgemäß festgelegte Aufgabenstellung zu verarbeiten oder zu nutzen. Die Übermittlung von Daten an Dritte darf nur im Rahmen der festgelegten Vertragszwecke erfolgen. Hierzu ist vorab weiterhin die Genehmigung des AG erforderlich.

2. Sollte der AN eine Übermittlung der personenbezogenen Daten an ein Drittland oder eine internationale Organisation vornehmen wollen, die nicht dem Recht der Europäischen Union oder der Mitgliedstaaten unterliegt, so muss dies der AG vorab genehmigen. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen dies und eventuelle rechtliche Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der AN darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter

Weisung des AG berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den AN wendet, wird der AN dieses Ersuchen unverzüglich an den AG weiterleiten. Der AG hat das Recht, dem AN jederzeit, insbesondere hinsichtlich der Art und des Zwecks der Datenverarbeitung, Weisungen zu erteilen. Der AN kann fordern, dass diese in Textform auf elektronischem Weg erteilt werden oder dass mündliche Weisungen durch den AG auf selbigem Wege bestätigt werden.

3. Der AN hat den AG unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Vorschriften der DSGVO oder gegen andere Datenschutzbestimmungen der Europäischen Union oder deren Mitgliedstaaten. Der AN ist dann berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis diese durch den AG bestätigt oder geändert wird.

§ 5 DATENÜBERMITTLUNG IN DRITTSTAATEN

Jede Verlagerung der vereinbarten Datenverarbeitung in ein Drittland bedarf der vorherigen Genehmigung des AG. Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet bis dahin ausschließlich in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt, es sei denn, der AG gestattet die Datenverarbeitung in einem Drittland vorab und der AN hat sich davon überzeugt, dass bei der datenverarbeitenden Stelle im Drittland ein erforderliches Schutzniveau für die Datenverarbeitung im Sinne des Art. 44 Satz 2 DSGVO vorliegt oder hergestellt wurde. Der AN garantiert für Verlagerungen der vereinbarten Datenverarbeitung in ein Drittland oder Hinzuziehung dort befindlicher Auftragsverarbeiter, dass die Einhaltung der besonderen Voraussetzungen der Art. 44 - 50 DSGVO erfüllt sind. Für die Zulässigkeit der Verlagerung in ein Drittland oder die Einbeziehung von Auftragsverarbeitern in einem Drittland trägt der AN die Verantwortung. Er hat die Zulässigkeit und die Einhaltung der DSGVO auf Verlangen des AG nachzuweisen. Werden seitens des AN mit der datenverarbeitenden Stelle Standarddatenschutzklauseln gemäß Art. 46 Abs. 2 lit. c) DSGVO zur Legitimation der Datenübermittlung geschlossen, so hat der Auftragsverarbeiter sicherzustellen, dass neben der Verwendung von Standarddatenschutzklauseln zudem zusätzliche Maßnahmen in Zusammenarbeit mit der datenverarbeitenden Stelle implementiert werden, um die Sicherstellung eines dem in der EU im Wesentlichen gleichwertigen Schutzniveaus zu gewährleisten.

§ 6 RÜCKGABE UND LÖSCHUNG DER DATEN

1. Kopien der Daten dürfen ohne Genehmigung des AG nicht erstellt werden. Hiervon ausgenommen sind Sicherheitskopien, soweit diese zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind. Der AN erwirbt keinerlei Rechte an den ihm zur Verfügung gestellten Daten, verwendet die Daten für keine anderen Zwecke als die ordnungsgemäße Durchführung des Vertrags und dieser Vereinbarung und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben.

2. Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den AG – spätestens nach Kündigung oder Erfüllung des Auftrags – hat der AN sämtliche in seinen Besitz gelangten digitalen Daten und Informationen sowie selbige in Papierform, die erstellten Verarbeitungs- und Nutzungsergebnisse sowie Daten und Informationen, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem AG auszuhändigen oder nach Wahl des AG datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist dem AG anschließend vorzulegen oder alternativ die Löschung in Textform zu bestätigen.

3. Der AN wird durch Abschluss dieser Vereinbarung zur Auftragsverarbeitung aufgefordert, die seitens des AG in der Anlage 3 definierten Löschregeln und -fristen entsprechend anzuwenden, um dem Wahlrecht des AG bezüglich der datenschutzgerechten Vernichtung der verarbeiteten Daten und Informationen nachzukommen.

Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den AN entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Der AN stellt sicher, dass diese Dokumentationen keine personenbezogenen Daten erhalten. Er kann sie zu seiner Entlastung bei Vertragsende dem AG übergeben.

§ 7 DATENSCHUTZBEAUFTRAGTE DES AN

Der AN gewährleistet, dass er einen Datenschutzbeauftragten benannt hat, insofern dieser gemäß § 38 Abs. 1 BDSG oder Art. 37 Abs. 1 DSGVO dazu verpflichtet ist, und dass der Datenschutzbeauftragte seine Tätigkeit gemäß § 38 Abs. 2 BDSG und Art. 38 und 39 DSGVO ausüben kann. Dessen Kontaktdaten werden dem AG oder dessen Datenschutzbeauftragten zum Zweck der direkten Kontaktaufnahme auf Anfrage unverzüglich mitgeteilt. Ein Wechsel des Datenschutzbeauftragten bzw. dessen Abberufung ist dem AG unverzüglich mitzuteilen.

§ 8 TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN ZUM SCHUTZ DER DATEN

1. Der AN gewährleistet die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 32 und Art. 5 Abs. 1 und 2 DSGVO. Diese hat der AN in der Anlage 2 zu diesem Vertrag zur Auftragsverarbeitung ausführlich darzulegen. Bei Akzeptanz durch den AG werden die dokumentierten Maßnahmen Grundlage des Auftrags.

2. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um solche der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der involvierten 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 gemäß Art. 32 Abs. 1 DSGVO zu berücksichtigen. Hierzu hat der AN insbesondere die Räume, in denen sich die Daten des AG befinden, so zu sichern, dass Unbefugten der Zutritt verwehrt wird, und sicherzustellen, dass der Zugriff auf die personenbezogenen Daten Unbefugten verwehrt wird. Er muss auch verhindern, dass die Unterlagen des AG von Unbefugten gelesen, verändert, kopiert oder entfernt werden können, und seine innerbetriebliche Organisation so gestalten, dass diese den besonderen Ansprüchen des Datenschutzes gerecht wird und die Daten nur im Rahmen der Weisungen des AG verarbeitet werden und während einer Übertragung ausreichend geschützt sind. Den für die Auftragsverarbeitung zuständigen Mitarbeitern des AN müssen diese Weisungen bekannt gemacht werden.

3. Der AN kontrolliert regelmäßig seine 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 Personen gewährleistet wird.

4. Der AN gewährleistet die Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem AG im Rahmen seiner Kontrollbefugnisse dieses Vertrags und wird dem AG diese, bei längerer Beauftragung, nach jährlicher Aufforderung erneut darlegen bzw. zusichern, dass sich keine Änderungen ergeben haben.

5. Soweit die Prüfung oder ein Audit des AG oder dessen Datenschutzbeauftragter oder ein Kontrollverfahren der zuständigen Aufsichtsbehörde einen Anpassungsbedarf der getroffenen Maßnahmen aufzeigt, ist dieser einvernehmlich umzusetzen.

6. Die getroffenen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem AN gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das vorherige Sicherheitsniveau nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

§ 9 EINBEZIEHUNG WEITERER AUFTRAGSVERARBEITER

1. Der AN darf keine weiteren Auftragsverarbeiter ohne vorherige nachweisliche und gesonderte Genehmigung des Verantwortlichen hinzuziehen. Der AN informiert den AG über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung genehmigter Auftragsverarbeiter, wodurch der AG die Möglichkeit erhält, die Änderung zu genehmigen.

2. Als hinzugezogene Auftragsverarbeiter im Sinne dieser Regelung sind solche Dienstleister zu verstehen, die sich unmittelbar ganz oder teilweise auf die Erbringung der beauftragten Datenverarbeitung beziehen. Nicht hierzu gehören Nebenleistungen, die der AN z. B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder zur Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der AN ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des AG auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

3. Zieht es der Auftragsverarbeiter in Erwägung, die Dienste eines weiteren Auftragsverarbeiters hinzuzuziehen, um bestimmte Verarbeitungstätigkeiten im Namen des AG auszuführen, so wird der AN diesem weiteren Auftragsverarbeiter im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Recht der Europäischen Union oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegen, die in diesem vorliegendem Vertrag zwischen AG und dem AN vereinbart sind, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so umgesetzt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt. Sämtliche Änderungen dieses Vertrags zur Auftragsverarbeitung hat der AN auch hinzugezogenen Auftragsverarbeitern fortwährend aufzuerlegen. Kommt der hinzugezogene Auftragsverarbeiter seinen Pflichten nicht nach oder verstößt dieser gegen die DSGVO, so haftet der AN gegenüber dem AG oder den betroffenen Personen für die Schäden, die dadurch entstanden sind.

4. Die Weitergabe von personenbezogenen Daten des AG an durch den AN hinzugezogene Auftragsverarbeiter ist erst mit Vorliegen der Genehmigung des AG über die Hinzuziehung und die Erfüllung aller Voraussetzungen aus § 9 des vorliegenden Vertrags erlaubt. Der AG erhält vom AN auf Aufforderung Einblick in die relevanten Vertragsunterlagen mit dem hinzugezogenen Auftragsverarbeiter, wobei der AN berechtigt ist, Preise und Vergütungen o. Ä. unkenntlich zu machen.

5. Soll der hinzugezogene Auftragsverarbeiter außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums tätig werden, stellt der AN die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Diese weist der AN dem AG unaufgefordert nach. Im Übrigen gilt § 5 dieses Vertrages.

6. Der AN hat die Auftragsverarbeiter, welche er hinzuzuziehen gedenkt, in Anlage 1 aufzulisten und die dort abgefragten Angaben zu beantworten. Durch Unterschrift dieses Vertrags zur Auftragsverarbeitung durch den AG wird deren Hinzuziehung genehmigt.

§ 10 KONTROLLBEFUGNISSE DES AG

1. Der AG ist gesetzlich verpflichtet, sich von der Einhaltung der in diesem Vertrag niedergelegten Pflichten, der Weisungen und der technischen und organisatorischen Maßnahmen im Sinne des § 7 beim AN zu überzeugen. Der AG hat das Recht, im Benehmen mit dem AN Überprüfungen durchzuführen oder durch die im Einzelfall zu benennenden Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieses Vertrags zur Auftragsverarbeitung durch den AN in dessen Geschäftsbetrieb zu überzeugen. Zu diesem Zweck darf das Betriebsgelände des AN im Beisein eines

Beauftragten des AN zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs durch den AG oder dessen Datenschutzbeauftragten betreten werden, damit sich von der Einhaltung der in diesem Vertrag niedergelegten Pflichten, der Weisungen und Umsetzung der Maßnahmen überzeugt werden kann.

2. Der AN stellt sicher, dass sich der AG oder dessen Datenschutzbeauftragter von der Erfüllung der datenschutzrechtlichen Pflichten des AN überzeugen kann. Der AN verpflichtet sich, dem AG 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 durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO oder die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO erfolgen. Wenn dem AG ausreichend, können hierzu auch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. von Wirtschaftsprüfern, Revision, Datenschutzbeauftragten, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudits verwendet werden.

4. Der AG kann bei Verstößen gegen den Datenschutz zusätzliche technische und organisatorische Maßnahmen fordern.

§ 11 UNTERSTÜTZUNGSPFLICHTEN DES AN

1. Der AG und der AN arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen. Soweit der AG 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 AN ausgesetzt ist, hat ihn der AN nach besten Kräften zu unterstützen.

2. Der AN unterstützt den AG angesichts der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte der betroffenen Personen nachzukommen. Der AN wird entsprechende Anträge nicht selbst bearbeiten bzw. beantworten, sondern diese unverzüglich an den AG weiterleiten.

3. Der AN stellt dem AG auf Anforderung alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung.

4. Der AN unterstützt den AG bei der Einhaltung der in den Art. 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgenabschätzungen und vorherigen Konsultationen. Hierzu gehören insbesondere:

die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, welche 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 Verpflichtung, Verletzung des Schutzes personenbezogener Daten unverzüglich an den AG zu melden,

- die Verpflichtung, den AG im Rahmen seiner Informationspflicht gegenüber den betroffenen Personen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevanten Informationen unverzüglich zur Verfügung zu stellen,
- die Unterstützung des AG bei der Erstellung von dessen Verzeichnis der Verarbeitungstätigkeiten, insofern sich dies auf die beauftragte Datenverarbeitung bezieht,

- die Unterstützung des AG für dessen Datenschutz-Folgenabschätzung und
- die Unterstützung des AG im Rahmen vorheriger Konsultationen der Aufsichtsbehörde.

Hierzu wird der AN dem AG auf Anforderung den Auszug seines Verzeichnisses der Verarbeitungstätigkeiten gemäß Art. 30 DSGVO zur Verfügung stellen, das sich auf die beauftragte Datenverarbeitung bezieht.

§ 12 INFORMATIONSPFLICHTEN DES AN

1. Der AN gewährleistet die unverzügliche Information des AG 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 AN ermittelt.

2. Sollten die Daten des AG bei dem AN durch Pfändung oder Beschlagnahmung, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden,
so hat der AN den AG unverzüglich darüber zu informieren. Der AN wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die „Hoheit und das Eigentum“ an den Daten ausschließlich beim AG als Verantwortlichem im Sinne der DSGVO liegen.

3. Der AN hat dem AG unverzüglich – auch bei bloßem Verdacht – alle Verletzungen der Sicherheit in seinem Haus, soweit diese Auswirkungen auf die Verarbeitung von personenbezogenen Daten des AG gehabt haben bzw. haben könnten, zu melden. Gemeldet werden müssen ferner alle Vorkommnisse, die Einfluss auf den Datenbestand des AG haben können (z. B. Einbrüche, Diebstähle, Feuerschäden usw.).

4. Der AN meldet dem AG unverzüglich alle Verstöße gegen diesen Vertrag zur Auftragsverarbeitung und gegen datenschutzrechtliche Vorschriften.

§ 13 VERSCHWIEGENHEIT UND WAHRUNG VON GESCHÄFTSGEHEIMNISSEN

1. Der AN hat sich mit der Geheimhaltung von Geschäftsgeheimnissen im Sinne des § 2 Nr. 1 des Gesetzes zum Schutz von Geschäftsgeheimnissen (GeschGehG) vertraut gemacht und sichert deren Einhaltung für sich und das durch ihn eingesetzte Personal sowie hinzugezogene Auftragsverarbeiter zu. Dies gilt auch für die sich aus dem vorliegenden Vertragsverhältnis ergebenden Folgeaufträge oder Auftragserweiterungen sowie andere künftige Geschäftsbeziehungen und bezieht sich auf alle Leistungen des AN gegenüber dem AG und ggf. dessen verbundene Unternehmen wie Mutter-, Tochter- und Schwestergesellschaften unabhängig davon, an welchem Ort diese erbracht werden. Sie erstrecken sich auf sämtliche personenbezogene Daten, Unternehmensdaten und -informationen, gleich in welcher Form diese vorliegen und gleich ob sie ausdrücklich als vertraulich bezeichnet sind oder nicht.

2. Der AN sichert zu, dass das von ihm eingesetzte Personal sämtliche während der Erfüllung des Auftrags auch zufällig zugänglich gewordenen Daten geheim hält, sich weder Aufzeichnungen darüber macht noch Kopien anfertigt, entsprechende Daten nicht an Dritte weitergibt oder für eigene Zwecke nutzt.

3. Sollte der AN bzw. dessen zur Vertragserfüllung eingesetztes Personal das E-Mail-System, das Internet/Intranet bzw. die IT-Systeme des AG nutzen wollen, so wird sich der AN bzw. das entsprechende Personal vorab die ausdrückliche Erlaubnis einholen und vor deren Nutzung beim AG über die internen Regelungen des AG zum Umgang mit diesen Systemen und Medien informieren und diesen entsprechen. Der AG behält sich vor, auf alle zur Verfügung gestellten Systeme sowie Daten und Informationen ohne Vorankündigung zuzugreifen. Der AN ist dann seinerseits verpflichtet, das von ihm eingesetzte Personal über die Einhaltung der genannten internen Regelungen des AG regelmäßig zu informieren und deren Einhaltung sicherzustellen.

4. Für eine Unterrichtung, Verpflichtung und Schulung des durch den AN eingesetzten Personals ist der AN verantwortlich. Der AN sichert zu, dass dieser nur Personal einsetzt, das mit den Anforderungen der DSGVO und allen nationalen sowie anderen einschlägigen Datenschutzbestimmungen, der Wahrung von Geschäftsgeheimnissen im Sinne des § 2 Nr. 1 GeschGehG, den Pflichten aus dieser Verpflichtungserklärung und zur Vertraulichkeit im Sinne des Art. 28 Abs. 3 Satz 2 lit. b)
DSGVO vertraut ist.

§ 14 SCHLUSSBESTIMMUNGEN

1. Der AN ist sich bewusst, dass die Verletzung dieses Vertrags zur Auftragsverarbeitung einen Verstoß gegen die DSGVO, das BDSG, das GeschGehG oder eine sonstige datenschutzrechtliche Vorschrift darstellen kann und dies eine Ordnungswidrigkeit oder Straftat darstellen kann und dass er für diese Verletzungen selbst verantwortlich sowie haftbar ist.

2. Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam sein oder werden, so wird die Wirksamkeit der übrigen Bestimmungen davon nicht berührt. An die Stelle der unwirksamen Bestimmungen wird eine andere treten, die wirksam ist und die nach Inhalt und Zweck der unwirksamen Bestimmung am nächsten kommt.

_____
Ort, Datum

_____
Aufraggeber

_____
Ort, Datum

_____
Auftragnehmer

ANLAGE 1: WEITERE AUFTRAGSVERARBEITER

Folgende Auftragsverarbeiter dürfen durch den AN im Rahmen der Tätigkeit, die in dem zu dieser Anlage gehörenden Vertrag zur Auftragsverarbeitung beschrieben ist, hinzugezogen werden:

WEITERER AUFTRAGSVERARBEITER NR. 1:

Name:

XXX

Anschrift inklusive Land:

XXX

Umfang, Art und Zweck der Tätigkeit:

XXX

WEITERER AUFTRAGSVERARBEITER NR. 2:

Name:

XXX

Anschrift inklusive Land:

XXX

Umfang, Art und Zweck der Tätigkeit:

XXX

WEITERER AUFTRAGSVERARBEITER NR. 3:

Name:

XXX

Anschrift inklusive Land:

XXX

Umfang, Art und Zweck der Tätigkeit:

XXX

WEITERER AUFTRAGSVERARBEITER NR. 4:
Name:

XXX

Anschrift inklusive Land:

XXX

Umfang, Art und Zweck der Tätigkeit:

XXX

WEITERER AUFTRAGSVERARBEITER NR. 5:
Name:
XXX

Anschrift inklusive Land:

XXX

Umfang, Art und Zweck der Tätigkeit:

XXX

WEITERER AUFTRAGSVERARBEITER NR. 6:
Name:

XXX

Anschrift inklusive Land:

XXX

Umfang, Art und Zweck der Tätigkeit:

XXX

ANLAGE 2: TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

1. VERTRAULICHKEIT

1.1 ZUTRITTSKONTROLLE

Ziel der Maßnahmen: Ein unbefugter Zutritt zu Datenverarbeitungsanlagen ist zu verhindern, wobei der Begriff räumlich zu verstehen ist. Geeignete technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten sind zu treffen.

Mögliche Beispiele für entsprechende Maßnahmen: Zutrittskontrollsystem, Ausweisleser, Magnetkarte, Chipkarte, Schlüssel/Schlüsselvergabe/sicheres Schließanlagensystem, Schließprotokoll, Türsicherung (elektrische Türöffner, Gegensprechanlage), Werkschutz, Wachhunde, Pförtner (Personenkontrolle, nächtlicher Sicherheitsdienst), Videoüberwachung des Geländes, Zutrittsberechtigungsregelungen für Mitarbeiter, Überwachungseinrichtung, Alarmanlage, Umzäunung, Video-/Fernsehmonitor, Schutz vor direkter unberechtigter Einsichtnahme von Monitoren durch Sichtschutz/Stellwände/Milchglasfolien, Polarisationsfolien für Bildschirme, Vermeidung von Datenverarbeitungen im Erdgeschoss, Bewegungsmelder, Anwesenheitsprotokollierung/Besucherlisten/Erfassung der Dienstleisterbesuche und Besucherausweise, Wahl eines risikoarmen Standorts, Ansiedlung der Datenverarbeitung in einem frei stehenden Gebäudekomplex, Zeitschlösser, Einrichtung von Sicherheitszonen und Sperrbereichen, Betrieb eines Closed-Shop-Systems, Personenvereinzelungsschleusen, Sicherheitsfenster, Spezialglas, Vergittern oder Weglassen von Fenstern, Sicherung von Schächten und Aufzügen, Sicherung von Kabelschächten und Verbindungen gegen elektrische Emissionen und Einwirkungen, Überwachung und Begleitung von Dienstleistern und Besuchern und zugehörige Stichprobenkontrollen.

Werden technische und organisatorische Maßnahmen zur Zutrittskontrolle unternommen?

☐ Ja ☐ Nein

Welche oder warum werden keine Maßnahmen ergriffen?

XXX

1.2 ZUGANGSKONTROLLE

Ziel der Maßnahmen: Das Eindringen Unbefugter in die IT-Systeme ist zu verhindern. Technische und organisatorische Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung sind erforderlich.

Mögliche Beispiele für entsprechende Maßnahmen: schriftliche Fixierung der Zugangsberechtigungen, Zuordnung von Benutzerprofilen zu Endgeräten, restriktive Vergabe von Zugangsberechtigungen, Regelung von Vertretungsberechtigungen, Einrichtung und Pflege einer elektronischen Benutzerverwaltung, Ausgestaltung der Passwörter möglichst nach Vorgaben des BSI (u. a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts), Erstellung einer Passwortrichtlinie in Form einer Dienstanweisung, Einrichtung eines Passwortschutzes für Hard- und Software, Passwortvergaberegelungen, automatische Sperrung (z. B. Kennwort, Pausenschaltung oder bei mehrfachen Fehlversuchen der Nutzung), Einrichtung eines Benutzerstammsatzes pro User, Verschlüsselung von Datenträgern, Erstellung von Protokollen über Aktivitäten der DV-Anlage/Auswertung der Protokolle zur Erkennung von Unregelmäßigkeiten, Verwendung von Magnet- oder Chipkarten/biometrischen Verfahren zur Authentifikation, Vermeidung von Fernzugriffen/Fernwartungen, Verwendung von Firewalls/Antivirensoftware, Verwendung von Endgeräten ohne Netzwerkanschluss (Stand-alone-Systeme), Einrichtung von Signaturverfahren zur Nutzeridentifizierung, Verwendung von abschließbaren Tastaturen und PCs sowie Nutzung von VPN.

Werden technische und organisatorische Maßnahmen zur Zugangskontrolle unternommen?

☐ Ja ☐ Nein

Welche oder warum werden keine Maßnahmen ergriffen?

XXX

1.3 ZUGRIFFSKONTROLLE

Ziel der Maßnahmen: Unerlaubte Tätigkeiten bzw. Einsichtnahmen in IT-Systeme(n) außerhalb eingeräumter Berechtigungen sind zu verhindern. Dazu sollte eine bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung vorgenommen werden.

Mögliche Beispiele für entsprechende Maßnahmen: Festlegung der Zuständigkeit bzgl. der Zugriffsrechtevergabe, ausreichend detaillierte, abgestufte und schriftliche Fixierung der Zugriffsrechte sowie Kommunikation selbiger an die jeweiligen Rechteinhaber, differenzierte Berechtigungen (Profile, Rollen, Transaktionen und Objekte), Protokollierung und Auswertung der Zugriffe und Zugriffsversuche, technische Einschränkung der Abfrage- und Zugriffsmöglichkeiten, Zuordnung von Zugriffsrechten zu Endgeräten und Benutzerprofilen, restriktive Vergabe der Zugangsberechtigungen, Regelung von Vertretungsberechtigungen, Einrichtung eines Passwortschutzes von Datensätzen bzw. Datengruppen, Regelung der Datenlöschung bzw. Datenträgervernichtung, richtige Archivierung von Daten/Verschlussmöglichkeiten, Regelung der Zugriffsrechte auf archivierte Daten, Nutzung des Mehraugenprinzips, Sperren von Datentransferschnittstellen, Verwendung von Magnet- oder Chipkarten/biometrischen Verfahren zur Authentifikation, automatische Zugriffssperren bei mehrfachen Fehlversuchen des Zugriffs.

Werden technische und organisatorische Maßnahmen zur Zugriffskontrolle unternommen?

☐ Ja ☐ Nein

Welche oder warum werden keine Maßnahmen ergriffen?

XXX

1.4 TRENNUNGSKONTROLLE

Ziel der Maßnahmen: Personenbezogene Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt und zweckgebunden zu verarbeiten. Maßnahmen zur getrennten Verarbeitung von Daten mit unterschiedlichen Zwecken sind erforderlich.

Mögliche Beispiele für entsprechende Maßnahmen: „Interne Mandantenfähigkeit“ (Kunden- bzw. Mandantentrennung), Zweckbindung, Dokumentation von Zwecken, zu denen die Daten erhoben wurden, Erstellung eines Berechtigungskonzepts, Erlass von Dienstanweisungen zur ausschließlich zweckgebundenen Datenverarbeitung, Deaktivierung von Möglichkeiten zur Exportierung von Daten aus Systemen, Unterbindung von Datenübermittlungen, Vergabe differenzierter Zugriffsrechte, Vergabe unterschiedlicher Rollen in Systemen, Trennung von Test- und Produktivdaten, Trennung der Daten nach Auftraggebern, Trennung der Zuordnungsdaten von pseudonymisierten Daten, Verschlüsselung der gespeicherten Daten und Speicherung von Daten in separierten Datenbanken/Datenbanksegmenten/Computerprogrammen.

Werden technische und organisatorische Maßnahmen zur Trennungskontrolle unternommen?

☐ Ja ☐ Nein

Welche oder warum werden keine Maßnahmen ergriffen?

XXX

1.5 PSEUDONYMISIERUNG

Ziel der Maßnahmen: Die Verarbeitung personenbezogener Daten ist in einer Weise vorzunehmen, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen zu deren Schutz unterliegen.

Mögliche Beispiele für entsprechende Maßnahmen: Pseudonymisierung durch Zuordnungstabellen, welche von der übrigen Datenverarbeitung getrennt sind, Erhobenen Daten werden
verschlüsselt abgespeichert und dem Datensatz wird ein kryptischer Wert (sogenannter Token)
zugeordnet mit dessen Hilfe eine weitere Verarbeitung ermöglicht wird.

Werden technische und organisatorische Maßnahmen zur Pseudonymisierung unternommen?

☐ Ja ☐ Nein

Welche oder warum werden keine Maßnahmen ergriffen?

XXX

1.6 AUFTRAGSKONTROLLE

Ziel der Maßnahmen: Die weisungsgemäße Auftragsdatenverarbeitung ist zu gewährleisten und technische sowie organisatorische Maßnahmen zur Abgrenzung der Kompetenzen zwischen AG und AN sind notwendig.

Mögliche Beispiele: eindeutige Vertragsgestaltung, formalisierte Auftragserteilung, Nutzung von Auftragsformularen, Kriterien zur Auswahl des Auftragnehmers, Erstellung und Aktualisierung einer Übersicht über die ergriffenen technischen und organisatorischen Maßnahmen, Abschluss eines schriftlichen Vertrags zur Auftragsverarbeitung mit den gesetzlichen Mindestinhalten sowie darüber hinausgehenden Informationen zur genauen Auftragsgestaltung, Zugänglichmachung des Vertrags zur Auftragsverarbeitung und der Weisungen für die involvierten Beschäftigten, Erteilung einer schriftlichen Anweisung zur Einhaltung der Weisungen des Auftraggebers, Schulung der Mitarbeiter auf die Anforderungen an den Datenschutz in Auftragsverarbeitungsverhältnissen, Verpflichtung der Beschäftigten auf Einhaltung des Datenschutzes, bei Bedarf Erstellung eines Fernwartungskonzepts, Abstimmung unpräziser oder unklarer Weisungen, Datenübergaben gegen Quittierungen, Prüfung der Identität und Weisungsbefugnis von unbekannten weisungsgebenden Personen, Verschlüsselung von Daten während der Übermittlung, Trennung der Daten verschiedener Mandanten, vollständige Löschung der Daten nach Auftragsabschluss und Datenübergabe, Regelung der Daten- bzw. Datenträgervernichtung, Definierung sicherer Transport- bzw. Übermittlungswege und ausschließliche Nutzung selbiger, Dokumentation der verschiedenen Schritte der Auftragsverarbeitung, sichere Aufbewahrung von Belegen/Dokumenten über die Verarbeitung der Daten, Stichprobenkontrollen über die Einhaltung der Weisungen durch Mitarbeiter, Zuordnung und ausschließliche Verwendung von Datenträgern je Auftraggeber und keine Verwendung von Echtdaten für Testzwecke.

Werden technische und organisatorische Maßnahmen zur Auftragskontrolle unternommen?

☐ Ja ☐ Nein

Welche oder warum werden keine Maßnahmen ergriffen?

XXX

1.7 VERSCHLÜSSELUNG

Ziel der Maßnahmen: Personenbezogene Daten sind durch eine Verschlüsselung vor der unbefugten Einsichtnahme Dritter zu schützen.

Mögliche Beispiele: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, unter anderem durch kryptografische Maßnahmen wie Virtual Private Networks (VPN), elektronische Signatur, Verschlüsselung mittels Hash-Wert (z. B. Blockchain-Technologie), Komprimierungsprogramme (z.B. 7Zip); Verschlüsselung der Hardware und Backup-Systeme.

Werden technische und organisatorische Maßnahmen zur Verschlüsselung unternommen?

☐ Ja ☐ Nein

Welche oder warum werden keine Maßnahmen ergriffen?

XXX

1.8 DATENSCHUTZFREUNDLICHE VOREINSTELLUNGEN

Ziel der Maßnahmen: Sicherstellung, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

Mögliche Beispiele: Der Verarbeitungsprozess ist so konzipiert, dass ausschließlich Daten
erhoben werden, die zur Ausführung der bestellten Leistung benötigt werden, Betroffene können selbst entscheiden, an wen die Daten offenbart werden sollen, die Daten können von Betroffenen eingesehen werden, eine Löschung kann durch den Betroffenen initiiert werden.

Werden technische und organisatorische Maßnahmen zur datenschutzfreundlichen Voreinstellung unternommen?

☐ Ja ☐ Nein

Welche oder warum werden keine Maßnahmen ergriffen?

XXX

2. INTEGRITÄT

2.1 WEITERGABEKONTROLLE

Ziel der Maßnahmen: Aspekte der Weitergabe von personenbezogenen Daten sind zu regeln in Hinsicht auf elektronische Übertragung, Datentransport und Übermittlungskontrolle. Ferner müssen Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträgern getroffen werden (manuell oder elektronisch).

Mögliche Beispiele: Aufzeichnung und Dokumentation aller durchgeführten und geplanten Übermittlungen mit Nennung des Empfängers, der Datenkategorien, des Übermittlungszwecks, des Absenders und des Datums sowie der Uhrzeit der Übermittlung, stichprobenartige Kontrolle der protokollierten Übermittlungen auf Zulässigkeit und Datenschutzkonformität, Erlass von Arbeitsanweisungen bzw. Richtlinien zur Datenträgernutzung und Datenübermittlung, Führen einer Übersicht der wiederkehrenden bzw. regelmäßigen Übermittlungen und deren Ablauf, ausschließliche Vergabe von Lese- und Schreibrechten für den jeweiligen PC-Nutzer, Einschränkung der Möglichkeit eines elektronischen Verbindungsaufbaus auf berechtigte Nutzer, Ausschluss der Verwendung von fremden bzw. unbekannten Datenträgern, Sperrung und Protokollierung der Schnittstellen der Datenverarbeitungsanlagen, Kontrolle der Empfangsadressen vor Versendung von Daten in Papierform oder per E-Mail bzw. per Fax, Schaffung der Möglichkeit zur Fernlöschung von mobilen Datenverarbeitungsanlagen, Nutzung von Wählleitungen mit automatischem Rückruf, Ende-zu-Ende-Verschlüsselung von Daten während einer elektronischen Übertragung bzw. Übermittlung, Nutzung eines VPN, Nutzung eines Content-Filters/einer Firewall, Verbot der Mitnahme oder des Mitbringens von privaten Datenträgern, datensichere Entsorgung von Daten und Datenträgern, elektronische Signatur, Protokollierung, Transportsicherung, Nutzung sicherer Transportfahrzeuge, Einrichten von Standleitungen und sicheren Netzen, Nutzung von Übertragungsprotokollen wie TLS/SSL oder SSH, Weitergabe der Daten möglichst in anonymisierter oder pseudonymisierter Form, Verbot der Speicherung sensibler Daten auf mobilen Datenträgern, Verschlüsselung/Passwortsicherung von Datenträgern, Identitätsprüfung von Empfängern und Taschenkontrollen.

Werden technische und organisatorische Maßnahmen zur Weitergabekontrolle unternommen?

☐ Ja ☐ Nein

Welche oder warum werden keine Maßnahmen ergriffen?

XXX

2.2 EINGABEKONTROLLE

Ziel der Maßnahmen: Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten. Maßnahmen zur nachträglichen Überprüfung, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt bzw. gelöscht worden sind, sind notwendig.

Mögliche Beispiele: Protokollierungs- und Protokollauswertungssysteme, Führung von manuellen Protokollen in Papierform, Protokollierung der Administratoraktivitäten über Systemprotokolle, Erlass von Dienstanweisungen und Schulung zur Eingabe/Veränderung/Entfernung von personenbezogenen Daten sowie deren Zulässigkeit, Auswertung von Protokollen in Zusammenarbeit mit dem betrieblichen/behördlichen Datenschutzbeauftragten und der Beschäftigtenvertretung, sichere Aufbewahrung der Protokolle, Erstellung von Sicherungskopien der Protokolle, Sammlung von Erfassungsbelegen, Führung eines Berechtigungskonzepts zur Eingabe/Veränderung/Entfernung von Daten, Zuordnen von Benutzern zu bestimmten Datenverarbeitungsanlagen, Protokollierung der Benutzeranmeldungen an Datenverarbeitungsanlagen, Protokollierung von erfolgreichen und gescheiterten Software-Log-ins, Protokollierung der Aktivitäten auf Servern und der Systemverwalter sowie Benutzer, Dokumentation von Eingabesoftware, Einrichtung von erforderlicher Identifikation zur Nutzung von Datenverarbeitungsanlagen und Software (z. B. durch Eingabe von Nutzername und Passwort oder Fingerabdruck), Einhaltung des Mehr-Augen-Prinzips, sichere Aufbewahrung

von Schichtplänen/Belegen/Dokumenten, Dokumentation von Stellvertreterregelungen sowie Abzeichnung der Belege und Dokumente und Richtigkeit über Stichprobenkontrollen.

Werden technische und organisatorische Maßnahmen zur Eingabekontrolle unternommen?

☐ Ja ☐ Nein

Welche oder warum werden keine Maßnahmen ergriffen?

XXX

3. VERFÜGBARKEIT UND BELASTBARKEIT

Ziel der Maßnahmen: Personenbezogene Daten sind gegen zufällige Zerstörung oder Verlust zu schützen. Maßnahmen zur Datensicherung müssen getroffen werden.

Mögliche Beispiele: Back-up-Verfahren, Spiegeln von Festplatten, z. B. RAID-Verfahren, unterbrechungsfreie Stromversorgung (USV), getrennte Aufbewahrung, Virenschutz, Firewall, Notfallplan, Berücksichtigung von möglichen Natureinflüssen, wie z. B. Hochwasser, Platzierung von Datenverarbeitungsanlagen in höheren Etagen, Installierung von Schutzsteckdosenleisten, Brandschutztüren, Alarmanlagen, Blitzableiter, Vergatterung von Fenstern, Einrichtung eines abgesicherten Stromanschlusses, Vermeidung der Nutzung von mobilen Endgeräten, galvanische Trennung von Netzwerkanschlüssen, keine Platzierung von Servern in Räumen mit Wasserleitungen in der Raumdecke, Synchronisierung von Daten, regelmäßiger Test der Funktion der Datensicherungen und der Einspielbarkeit der gesicherten Daten, Kühlung und Belüftung von Servern, Bereitstellung von Feuerlöschern, Installierung von Brandmeldern, Durchführung von Brandschutzbegehungen, Installierung von Brandfrüherkennungsanlagen, schriftliche Fixierung eines Datensicherheitskonzepts, Erteilung einer schriftlichen Dienstanweisung zur Sicherung von Daten auf mobilen Geräten/Datenträgern, Schulung der Mitarbeiter auf den richtigen Umgang mit Datenverarbeitungsanlagen/Speichermedien/Datensicherungen, Erstellung eines Katastrophenplans, Auslagerung von Datensicherungen bei zertifizierten Dienstleistern, Umkopieren der Daten von Speichermedien mit begrenzter Lebensdauer wie z. B. CD-ROM/DVD auf andere Datenträger, Aufbewahrung von Datensicherungen in feuerfesten Tresoren, betriebliches Rauchverbot, Durchführung von internen Überprüfungen der Belastbarkeit und Belastung der Systeme sowie Durchführung von IT-Penetrationstests durch einen externen Dienstleister.

Werden technische und organisatorische Maßnahmen zur Verfügbarkeitskontrolle unternommen?

☐ Ja ☐ Nein

Welche oder warum werden keine Maßnahmen ergriffen?

XXX

4. ORGANISATORISCHE MAßNAHMEN

Ziel der Maßnahmen: die Mitarbeiter über den richtigen Umgang mit Daten zu informieren, anzuweisen und erforderliche Vorgehensweise zu definieren, um die Daten ausreichend zu schützen.

Mögliche Beispiele: regelmäßige Mitarbeiterschulungen mit Nachweis, Sicherheitskonzept, schriftlich unterschriebene Verpflichtung auf das Datengeheimnis, schriftliche Arbeitsanweisungen, Betriebsvereinbarungen, Richtlinien oder Merkblätter zum Datenschutz, schriftliche Dokumentation zum Ein- oder Austritt ins Unternehmen, schriftlich geregelte und dokumentierte Schlüsselvergabe, Dokumentation von

Auskunftsersuchen, Anliegen, Berichtigungen, Löschungen oder Sperrungen von personenbezogenen Daten, manuell geführte Protokolle, schriftliche Einwilligung, Verpflichtung aller Dienstleister auf den Datenschutz, Nutzung von Schweigepflichtentbindung, Prüfungen durch die interne oder externe Revision, Riskmanager, Compliance Officer, IT-Sicherheitsbeauftragten, Qualitätsmanager, etablierte Meldeprozesse für Datenschutzverstöße und Incident-Response-Management für IT-Sicherheitsvorfälle, Durchführen von internen und externen Audits, Erlangung einer Datenschutzzertifizierung, Definition und Einhaltung von Verhaltensregelungen und Selbstverpflichtungen.

Werden grundsätzlich organisatorische Maßnahmen unternommen?

☐ Ja ☐ Nein

Welche oder warum werden keine Maßnahmen ergriffen?

XXX

5. KONTROLLEN DER TECHNISCHEN UND ORGANISATORISCHEN MAßNAHMEN

Ziel der Maßnahmen: ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Mögliche Beispiele: regelmäßige Stichprobenkontrollen, anlassbezogene Kontrollen, Sichtung und Auswertung von Protokoll- und Logdateien, Sichtung von manuellen Protokollen und Listen, Prüfungen durch den Datenschutzbeauftragten, die interne oder externe Revision, Riskmanager, Compliance Officer, IT-Sicherheitsbeauftragten, Qualitätsmanager, etablierte Meldeprozesse für Datenschutzverstöße und Incident-Response-Management für IT-Sicherheitsvorfälle, Durchführen von internen und externen Audits, Durchführung von Mitarbeiter-, Dienstleister- oder Kundenumfragen zum Status des Datenschutzes, Erlangung einer Datenschutzzertifizierung.

Werden grundsätzlich organisatorische Maßnahmen unternommen?

☐ Ja ☐ Nein

Welche oder warum werden keine Maßnahmen ergriffen?

XXX

ANLAGE 3: WEISUNG DES AUFTRAGGEBERS AN DEN AUFTRAGNEHMER ZUR DATENLÖSCHUNG

Der AN verarbeitet im Auftrag des AG folgende Datenkategorien und löscht diese nach folgenden Regeln:

Nr.	Datenkategorien	Löschregel
1		
2		
3		
4		
5		

Der AN stellt sicher, dass er die Dokumentation der Löschläufe nach § 6 für Zwecke der Datenschutzprüfung mindestens 3 Jahre rückwirkend nachweisen kann. Soweit andere rechtliche Vorschriften einschlägig sind, beispielsweise die Abgabenordnung, sind die Dokumentationen gegebenenfalls entsprechend länger vorzuhalten.

Durch Unterschrift werden die Richtigkeit der gemachten Angaben und die Einhaltung der geschilderten technischen und organisatorischen Maßnahmen garantiert.

_____
Ort, Datum

_____
Auftragnehmer