

## Vertrag zur Auftragsverarbeitung

Zwischen

---

---

---

---

als Verantwortlicher (hier bezeichnet als „Auftraggeber“)

und

---

---

---

---

als Auftragsverarbeiter (hier bezeichnet als „Auftragnehmer“)

### Präambel

Der Auftraggeber möchte den Auftragnehmer mit den in § 3 genannten Leistungen beauftragen. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten. Insbesondere Art. 28 DSGVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien die nachfolgende Vereinbarung, deren Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

## **§ 1 Begriffsbestimmungen**

(1) Verantwortlicher ist gem. Art. 4 Abs. 7 DSGVO die Stelle, die allein oder gemeinsam mit anderen Verantwortlichen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

(2) Auftragsverarbeiter ist gem. Art. 4 Abs. 8 DSGVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

(3) Personenbezogene Daten sind gem. Art. 4 Abs. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

(4) Besonders schutzbedürftige personenbezogene Daten sind personenbezogenen Daten gem. Art. 9 DSGVO, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit von Betroffenen hervorgehen, personenbezogene Daten gem. Art. 10 DSGVO über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungs- maßregeln sowie genetische Daten gem. Art. 4 Abs. 13 DSGVO, biometrischen Daten gem. Art. 4 Abs. 14 DSGVO, Gesundheitsdaten gem. Art. 4 Abs. 15 DSGVO sowie Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

(5) Verarbeitung ist gem. Art. 4 Abs. 2 DSGVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

(6) Aufsichtsbehörde ist gem. Art. 4 Abs. 21 DSGVO eine von einem Mitgliedstaat gem. Art. 51 DSGVO eingerichtete unabhängige staatliche Stelle.

## **§ 2 Zusammenarbeit mit Datenschutzaufsichtsbehörde**

Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

### **§ 3 Vertragsgegenstand**

(1) Der Auftragnehmer erbringt für den Auftraggeber Leistungen im Bereich Videoüberwachung auf Grundlage des Vertrags vom \_\_\_\_\_ („Hauptvertrag“). Dabei erhält der Auftragnehmer Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers. Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer ergeben sich aus dem Hauptvertrag. Dem Auftraggeber obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung.

(2) Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung. Die Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Hauptvertrags vor.

(3) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei der der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden.

(4) Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüber hinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

### **§ 4 Weisungsrecht**

(1) Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Auftraggebers erheben, verarbeiten oder nutzen; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.

(2) Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten.

Die weisungsberechtigten Personen sind folgende Personen:

Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen ist dem Vertragspartner unverzüglich der Nachfolger bzw. Vertreter in Textform zu benennen.

(3) Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

(4) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

### **§ 5 Art der verarbeiteten Daten, Kreis der Betroffenen**

(1) Im Rahmen der Durchführung des Hauptvertrags erhält der Auftragnehmer Zugriff auf die in Anlage 1 näher spezifizierten personenbezogenen Daten. Diese Daten umfassen die Videoaufnahmen, insbesondere das Aussehen und die äußerliche Erscheinung einer Person.

(2) Der Kreis der von der Datenverarbeitung Betroffenen sind Mitarbeiter, Kunden und potentielle Kunden sowie Geschäftspartner des Auftraggebers.

### **§ 6 Schutzmaßnahmen des Auftragnehmers**

(1) Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DSGVO, insbesondere mindestens die in Anlage 1 aufgeführten Maßnahmen.

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Beim Auftragnehmer ist als betrieblicher Datenschutzbeauftragter/als Ansprechpartner für den Datenschutz (sofern ein Datenschutzbeauftragter nach Art. 37 Abs. 1 DSGVO nicht bestellt werden muss) bestellt:

Der Auftragnehmer veröffentlicht die Kontaktdaten des Datenschutzbeauftragten auf seiner Internetseite und teilt sie der Aufsichtsbehörde mit. Veröffentlichung und

Mitteilung weist der Auftragnehmer auf Anforderung des Auftraggebers in geeigneter Weise nach.

(4) Den bei der Datenverarbeitung durch den Auftragnehmer beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Der Auftragnehmer wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im folgenden Mitarbeiter genannt), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DSGVO) und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Mitarbeiter und dem Auftragnehmer bestehen bleiben. Dem Auftraggeber sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.

## **§ 7 Informationspflichten des Auftragnehmers**

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich in Schriftform oder Textform informieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest folgende Informationen:

- a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;
- b) eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(2) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen, informiert hierüber den Auftraggeber und ersucht um weitere Weisungen.

(3) Der Auftragnehmer ist darüber hinaus verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Absatz 1 betroffen sind.

(4) 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, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass

die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als „Verantwortlichem“ im Sinne der DSGVO liegen.

(5) Über wesentliche Änderung der Sicherheitsmaßnahmen nach § 6 Abs. 2 hat der Auftragnehmer den Auftraggeber unverzüglich zu unterrichten.

(6) Ein Wechsel in der Person des betrieblichen Datenschutzbeauftragten/Ansprechpartners für den Datenschutz ist dem Auftraggeber unverzüglich mitzuteilen.

(7) Der Auftragnehmer und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 DSGVO enthält. Das Verzeichnis ist dem Auftraggeber auf Anforderung zur Verfügung zu stellen.

(8) An der Erstellung des Verfahrensverzeichnisses durch den Auftraggeber hat der Auftragnehmer im angemessenen Umfang mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

## **§ 8 Kontrollrechte des Auftraggebers**

(1) Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers. Hierfür kann er z. B. Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören.

(2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen mündliche oder schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragnehmers erforderlich sind.

(3) Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

(4) Der Auftragnehmer stellt dem Auftraggeber auf dessen Wunsch ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsverarbeitung sowie über zugriffsberechtigte Personen zur Verfügung.

(5) Der Auftragnehmer weist dem Auftraggeber die Verpflichtung der Mitarbeiter nach § 6 Abs. 4 auf Verlangen nach.

## **§ 9 Einsatz von Subunternehmern**

(1) Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen nicht zur Begründung von Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis“) befugt.

(2) Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Subunternehmerverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

## **§ 10 Anfragen und Rechte Betroffener**

(1) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12–22 sowie 32 und 36 DSGVO.

(2) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, so reagiert dieser nicht selbstständig, sondern verweist den Betroffenen unverzüglich an den Auftraggeber und wartet dessen Weisungen ab.

## **§ 11 Haftung**

(1) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zum Auftragnehmer alleine der Auftraggeber gegenüber dem Betroffenen verantwortlich.

(2) Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist.

## **§ 12 Außerordentliches Kündigungsrecht**

(1) Der Auftraggeber kann den Hauptvertrag fristlos ganz oder teilweise kündigen, wenn der Auftragnehmer seinen Pflichten aus diesem Vertrag nicht nachkommt, Bestimmungen der DSGVO vorsätzlich oder grob fahrlässig verletzt oder eine Weisung des Auftraggebers nicht ausführen kann oder will. Bei einfachen – also weder

vorsätzlichen noch grob fahrlässigen – Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist, innerhalb welcher der Auftragnehmer den Verstoß abstellen kann.

### **§ 13 Beendigung des Hauptvertrags**

(1) Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder – auf Wunsch des Auftraggebers, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Der Auftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Daten zu führen. Zu entsorgende Unterlagen sind mit einem Aktenvernichter nach DIN 32757-1 zu vernichten. Zu entsorgende Datenträger sind nach DIN 66399 zu vernichten.

(2) Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren.

(3) Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus solange gültig, wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm vom Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat.

### **§ 14 Schlussbestimmungen**

(1) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i. S. d. § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

(3) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

(4) Diese Vereinbarung unterliegt deutschem Recht.

---

Datum und Unterschriften

Anlagen – Technische und organisatorische Maßnahmen des Auftragnehmers



## **Anlage 1**

### **Technische und organisatorische Maßnahmen**

Im Folgenden werden die technischen und organisatorischen Maßnahmen beschrieben, die der Auftragnehmer zur Gewährleistung von Datenschutz und Datensicherheit ergriffen hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der durch den Auftragnehmer verarbeiteten personenbezogenen Daten.

*[Bitte Zutreffendes ankreuzen und ggf. weitere vorhandene technische und organisatorische Maßnahmen ergänzen.]*

### **Informationen zum Standort von Datenverarbeitungsanlagen und Rechenzentren**

Der Standort des Rechenzentrums (hauptsächlich Hosting und E-Mail-Server) liegt bei der 1&1 Internet SE. Die Serverstandorte befinden sich in Deutschland. Weitere Datenverarbeitungen finden in-House statt, ein eigenes Rechenzentrum wird allerdings nicht betrieben. *(Bitte entsprechend einsetzen)*

#### **1. Vertraulichkeit (Art. 32 Abs. 1 lit. b)**

##### **(1) Zutrittskontrolle**

Maßnahmen, damit Unbefugte keinen Zutritt zu den Datenverarbeitungsanlagen erhalten, mit denen personenbezogene Daten verarbeitet werden.

- ☐ Die Datenverarbeitungsanlagen, mit deren Hilfe Daten des Auftraggebers verarbeitet werden, befinden sich in separaten abgeschlossenen Räumen, zu denen nur befugte Personen ein Zutrittsrecht besitzen.
- ☐ Der Zutritt zu den Datenverarbeitungsanlagen ist durch Magnet- oder Chipkarten gesichert. Der Zutritt wird protokolliert.
- ☐ Außenfenster sind durch besondere Schutzmaßnahmen gesichert.
- ☐ Räume sind durch eine Alarmanlage gesichert.
- ☐ Der Zutritt zu den Räumen wird videoüberwacht.

##### **(2) Zugangskontrolle**

Maßnahmen, damit Unbefugte an der Benutzung der Datenverarbeitungsanlagen gehindert werden:

- ☐ Die Nutzung der Datenverarbeitungssysteme und -programme ist nur durch autorisierte Benutzer möglich, die eine entsprechende Zugangsberechtigung besitzen.
- ☐ PCs werden bei längerer Inaktivität des Nutzers automatisch gesperrt.
- ☐ Autorisierte Benutzer sind angehalten, ihre Zugangsdaten geheim zu halten und diese Dritten nicht zugänglich zu machen.

- ☐ Es bestehen Mindeststandards für Passwörter. Passwörter sind darüber hinaus regelmäßig zu ändern.
- ☐ Für besonders sensible Datenverarbeitungsverfahren ist eine Anmeldung mittels Zwei-Faktor-Authentifizierung erforderlich.
- ☐ Daten werden mittels sicherer Löschroutinen gelöscht.
- ☐ Datenträger werden verschlüsselt.

### **(3) Zugriffskontrolle**

Maßnahmen, damit die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können sowie weitere Maßnahmen, mit denen die Vertraulichkeit der Systeme und Dienste sichergestellt ist:

- ☐ Es bestehen Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte. Für die Sicherstellung der ausschließlich befugten Benutzung sind für die Anwender entsprechende abgestufte Zugriffsberechtigungen auf Programm- bzw. Ordnerbene im EDV-Netzwerk eingerichtet.
- ☐ Zugriffe und Dateiänderungen werden protokolliert. Die Protokolle selbst unterliegen einer regelmäßigen Kontrolle.

### **(4) Trennungskontrolle**

Maßnahmen, die sicherstellen, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt voneinander verarbeitet werden können:

- ☐ Die Trennung der Daten des Auftraggebers von eigenen Daten erfolgt durch physikalische Trennung der Datenverarbeitungssysteme.
- ☐ Die Trennung der Daten des Auftraggebers von eigenen Daten erfolgt durch logische Trennung der Datenverarbeitungssysteme im Rahmen des Berechtigungskonzepts.

### **(5) Pseudonymisierung (Art. 32 Abs. 1 lit. a; Art. 25 Abs. 1)**

- ☐ Die Trennung 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 entsprechenden technischen und organisatorischen Maßnahmen unterliegen:

## **2. Integrität (Art. 32 Abs. 1 lit. b)**

### **(1) Datenverarbeitungskontrolle und Weitergabekontrolle inkl. Kontrolle zur dauerhaften Integrität der Systeme und Dienste**

Maßnahmen, damit personenbezogene Daten nicht unbefugt oder nicht zufällig gespeichert, zur Kenntnis genommen, verändert, kopiert, gelöscht, entfernt, vernichtet oder sonst verarbeitet werden sowie Maßnahmen zur Überprüfung und Feststellung an welchen Stellen die personenbezogenen Daten mit Hilfe von Datenübertragungsvorrichtungen übermittelt werden sollen oder worden sind:

- ☐ Entsprechend der Aufgabenerfüllung sind für die zugriffsberechtigten Beschäftigten abgestufte Zugriffsberechtigungen auf Programm- bzw. Ordner Ebene im EDV-Netzwerk eingerichtet, um bei der Verarbeitung oder Nutzung der Daten deren unbefugtes Lesen, Kopieren, Verändern, Entfernen oder deren Übermittlung zu verhindern.
- ☐ Daten werden mittels gesicherter Verfahren elektronisch übertragen und transportiert. Datenübermittlungen werden protokolliert.
- ☐ Die bestehenden Sicherheitssysteme werden regelmäßig überwacht. Im Falle von Sicherheitsmeldungen findet eine automatische Eskalation statt.
- ☐ Wechseldatenträger (wie USB-Sticks, CDs, DVDs, Blu-ray, externe Festplatte) sind nach aktuellem Stand der Technik verschlüsselt.
- ☐ Die E-Mail-Korrespondenz ist nach TLS 1.2 verschlüsselt.
- ☐ Nutzung von Virtual Private Networks (VPN) für externe Zugriffe auf das Firmennetzwerk.

### **(2) Eingabekontrolle**

Maßnahmen, um festzustellen, ob und von wem welche personenbezogenen Daten zu welcher Zeit in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

- ☐ Datenverarbeitungsvorgänge werden protokolliert.
- ☐ Veränderungen von Dokumenten werden über ein Dokumentenmanagementsystem protokolliert.
- ☐ Protokolle werden regelmäßig kontrolliert und ausgewertet.

## **3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b)**

### **(1) Verfügbarkeitskontrolle**

Maßnahmen zum Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust von Daten:

- ☐ Backup-Strategie (online/offline; on-site/off-site)
- ☐ Unterbrechungsfreie Stromversorgung (USV)
- ☐ Eine zentrale Firewall, die von einem Virens Scanner unterstützt wird, schützt das Unternehmensnetzwerk vor unberechtigtem Zugriff von außen und

überwacht die jeweilige Verbindung. PCs, die über einen Zugang nach außen verfügen (externe Medien, Internet, E-Mail), sind zusätzlich mit einem lokalen Virens Scanner ausgestattet.

- ☐ Meldewege und Notfallpläne
- ☐ Datenverarbeitungssysteme unterliegen regelmäßigen Sicherheitsupdates.

**(2) Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c)**

Die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen:

- ☐ Backup-Strategie (online/offline; on-site/off-site) (siehe oben)

**4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung (Art. 32 Abs. 1 lit. d; Art. 25 Abs. 1, 2)**

Maßnahmen, zur Überprüfung, Bewertung und Evaluierung der Wirksamkeit dieser technischen und organisatorischen Maßnahmen:

- ☐ Die getroffenen technischen und organisatorischen Maßnahmen werden regelmäßig im Hinblick Wirksamkeit und Aktualität kontrolliert.
- ☐ Die regelmäßige Überprüfung, Bewertung und Evaluierung wird protokolliert.
- ☐ Im Fall von Sicherheitsmeldungen findet eine automatische Eskalation an die verantwortlichen Mitarbeiter statt.
- ☐ Es besteht eine Richtlinie zum Umgang mit Sicherheitsmeldungen und (möglichen) Datenschutzverstößen.

**5. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2)**

Maßnahmen, um sicherzustellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist.

- ☐ Über Eingabemasken werden nur die Daten abgefragt, die für den jeweiligen Verarbeitungszweck erforderlich sind.
- ☐ Zugriff auf Daten gemäß Berechtigungskonzept.
- ☐ Begrenzung der Speicherfrist durch Löschkonzept.

## **6. Auftragskontrolle**

Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers:

- ☐ Eindeutige Vertragsgestaltung
- ☐ Formalisiertes Auftragsmanagement
- ☐ Strenge Auswahl des Dienstleisters
- ☐ Vorabüberzeugungspflicht
- ☐ Nachkontrollen

## **7. Organisationskontrolle**

Maßnahmen, damit die oder innerbetriebliche Organisation den besonderen Anforderungen des Datenschutzes gerecht wird:

- ☐ Sämtliche Beschäftigten (einschließlich Auszubildende und Praktikanten) und externen Dienstleister sind auf die Einhaltung der datenschutzrechtlichen Anforderungen nach der DSGVO sowie auf das Datengeheimnis nach § 53 BDSG verpflichtet.
- ☐ Die Beschäftigten werden regelmäßig im erforderlichen Maß datenschutzrechtlich geschult.