starfinanz

Auftragsverarbeitungsvertrag („AVV“)

zwischen

Testfirma

Name

Teststr. 1

12345 Teststadt, Deutschland

Anschrift

(kurz: „**Auftraggeber**“)

Und

Star Finanz-Software Entwicklung und Vertriebs GmbH, Grüner Deich 15, 20097 Hamburg
(kurz: „**Auftragnehmer**“)

Auftraggeber und Auftragnehmer werden einzeln bzw. gemeinsam auch als „Partei“ bzw. „Parteien“ bezeichnet

1. Gegenstand der Verarbeitung (des Auftrags)

Gegenstand des Auftrags ist: Umsetzung der beauftragten Support-Leistung.

2. Dauer des Auftrags

Die Dauer des Auftrags ergibt sich aus der schriftlich beauftragten Supportleistung.

3. Zweck der Verarbeitung

Die Tätigkeit des Auftragnehmers dient folgenden vereinbarten Zwecken:

Umsetzung der beauftragten Support-Leistung.

Folgende Datenarten können Gegenstand dieses Auftrags sein:

- Adressdaten
- Bankverbindungsdaten inkl. Zahlungsverkehrsdaten
- E-Mails
- Kreditkartendaten
- Lohn- und Gehaltsdaten
- Namen
- Nutzerkennungen

- Passwörter
- Telefonnummern
- Zahlungsdaten
- Zugangsdaten
- sonstige: Ggfs. alle, die beim Aufraggeber gespeicherten und die für die Abwicklung des Auftrags benötigten Daten

4. Kreis der Betroffenen

Folgende Kategorien von Betroffenen können Gegenstand des Auftrags sein:

- Beschäftigte
- Auszubildende und Praktikanten
- freie Mitarbeiter
- Kunden
- Lieferanten und Dienstleister
- Geschäftspartner
- sonstige: Ggfs. alle, die mit dem Aufraggeber geschäftlich zusammenarbeiten

5. Verantwortlichkeit und Verarbeitung auf Weisung

5.1. Der Auftraggeber ist im Rahmen dieses AVV für die Einhaltung der anwendbaren gesetzlichen Bestimmungen zum Datenschutz, insbesondere für die Rechtmäßigkeit der Offenlegung gegenüber dem Auftragnehmer sowie für die Rechtmäßigkeit der Verarbeitung allein verantwortlich („Verantwortlicher“ im Sinne des Art. 4 Nr. 7 DSGVO).

5.2. Der Auftragnehmer handelt ausschließlich weisungsgebunden, außer es liegt ein Ausnahmefall im Sinne des Art. 28 Abs. 3 a DSGVO vor (anderweitige gesetzliche Verarbeitungspflicht). Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

5.3. Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten oder schränkt deren Verarbeitung ein (kurz: „Sperrung“), wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist.

5.4. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Vorschriften über den Datenschutz verstößt. Der Auftragnehmer darf die Umsetzung der Weisung so lange aussetzen, bis diese vom Auftraggeber in Textform bestätigt oder abgeändert wurde. Die Ausführung offensichtlich datenschutzrechtswidriger Weisungen darf der Auftragnehmer jederzeit ablehnen.

5.5. Der Auftragnehmer gewährleistet, dass die zur Verarbeitung der Daten befugten Personen die Weisungen des Auftraggebers kennen und diese beachten.

5.6. Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung der Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits- und Verschwiegenheitspflicht besteht auch nach Beendigung der Verarbeitung fort.

5.7. Der Auftragnehmer hat bei der Verarbeitung im Auftrag das Bankgeheimnis zu wahren, soweit der Auftraggeber dem Bankgeheimnis unterworfen ist. Hierauf wird der Auftraggeber den Auftragnehmer hinweisen, sofern dies für den Auftragnehmer aus dem Hauptvertrag nicht ersichtlich ist. Das Bankgeheimnis erstreckt sich auf alle personenbezogenen Daten und anderen Informationen, die dem Auftraggeber über seine Kunden, Interessenten oder über Dritte aus der Geschäftsbeziehung zu diesen

bekannt werden. Unter das Bankgeheimnis fällt auch die Angabe, ob der Auftraggeber überhaupt eine Geschäftsbeziehung zu einem Kunden unterhält.

6. Sicherheit der Verarbeitung

6.1. Die Parteien vereinbaren technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO zum angemessenen Schutz der Daten (kurz: „TOM“), welche in diesem AVV aufgeführt sind.

6.2. Änderungen der vereinbarten TOM bleiben dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau insgesamt nicht unterschritten wird. Wesentliche Änderungen sind dem Auftraggeber in Textform mitzuteilen.

7. Unterrichtung bei Datenschutzverletzungen und Fehlern der Verarbeitung

7.1. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes der ihm vom Auftraggeber offengelegten Daten im Sinne des Art. 4 Nr. 12 DSGVO in seinem Organisationsbereich bekannt werden oder ein konkreter Verdacht einer solchen Datenschutzverletzung beim Auftragnehmer besteht.

7.2. Stellt der Auftraggeber Fehler bei der Verarbeitung fest, hat er den Auftragnehmer unverzüglich hierüber zu unterrichten.

7.3. Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Behebung der Datenschutzverletzung gemäß Ziffer 8.1 oder der Fehler gemäß Ziffer 8.2 sowie zur Minderung möglicher nachteiliger Folgen, insbesondere für die betroffenen Personen. Hierüber stimmt er sich mit dem Auftraggeber ab. Mündliche Unterrichtungen gemäß Ziffer 8.1 oder Ziffer 8.2 sind unverzüglich in Textform nachzureichen.

8. Übermittlung von Daten an einen Empfänger in einem Drittland

Eine Offenlegung und/oder Übermittlung von Daten an Empfänger in Drittländern erfolgt nicht.

9. Unterbeauftragung weiterer Auftragsverarbeiter

9.1. Der Auftragnehmer darf die Verarbeitung personenbezogener Daten ganz oder teilweise durch weitere Auftragsverarbeiter (kurz: „**Unterauftragnehmer**“) erbringen lassen.

9.2. Der Auftragnehmer informiert den Auftraggeber in Textform rechtzeitig vorab über die Beauftragung von weiteren Unterauftragnehmern oder Änderungen in der Unterbeauftragung. Der Auftraggeber kann bei Vorliegen eines wichtigen Grundes der Unterbeauftragung innerhalb von vier Wochen nach Kenntnisnahme in Textform widersprechen. Ein wichtiger Grund liegt insbesondere vor, wenn ein begründeter Anlass zu Zweifeln besteht, dass der Unterauftragnehmer die vereinbarte Leistung entsprechend den anwendbaren gesetzlichen Bestimmungen zum Datenschutz oder gemäß dieser AVV erbringt.

9.3. Der Auftragnehmer wird mit dem Unterauftragnehmer die in diesem AVV getroffenen Regelungen inhaltsgleich vereinbaren. Insbesondere müssen die mit dem Unterauftragnehmer zu vereinbarenden technischen und organisatorischen Maßnahmen mindestens dasselbe Schutzniveau aufweisen.

9.4. Keine Unterbeauftragungen im Sinne dieser Regelung sind Leistungen, die der Auftragnehmer als reine Nebenleistung zur Unterstützung seiner geschäftlichen Tätigkeit außerhalb der Auftragsverarbeitung

in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes der Daten auch für solche Nebenleistungen angemessene Vorkehrungen zu ergreifen.

10. Sonderkündigungsrecht des Auftraggebers bei Widerspruch der beauftragenden Stelle

Erfolgt die Beauftragung des Auftragnehmers als Unterauftragsverarbeitung des Auftraggebers, so steht der beauftragenden Stelle des Auftraggebers ein Widerspruchsrecht nach Art. 28 (2) DSGVO zu. Dieses Widerspruchsrecht besteht für einen Zeitraum von 4 Wochen ab Kenntnisnahme der beauftragenden Stelle über die Unterbeauftragung des Auftragnehmers. Sollte die beauftragende Stelle binnen der vorgenannten Frist von diesem Widerspruchsrecht gegenüber dem Auftraggeber Gebrauch machen, so steht dem Auftraggeber ein fristloses Sonderkündigungsrecht dieses Vertrages und der zugehörigen Beauftragung des Auftragnehmers zu.

11. Rechte betroffener Personen und Unterstützung des Auftraggebers

Macht eine betroffene Personen Ansprüche gemäß Kapitel III der DSGVO bei einer der Parteien geltend, so informiert sie die jeweils andere Partei darüber unverzüglich. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Bearbeitung solcher Anträge sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten.

12. Kontroll- und Informationsrechte des Auftraggebers

12.1. Der Auftragnehmer weist dem Auftraggeber die Einhaltung seiner Pflichten mit geeigneten Mitteln nach. Der Auftraggeber überprüft die Geeignetheit.

12.2. Für die Überprüfung der Einhaltung der vereinbarten Schutzmaßnahmen nach Ziffer 13.1. und deren geprüfter Wirksamkeit kann der Auftragnehmer auf angemessene Zertifizierungen oder andere geeignete Prüfungsnachweise verweisen. Angemessen sind insbesondere Zertifizierungen nach Art. 40 DSGVO oder Nachweise nach Art. 42 DSGVO. Daneben kommen unter anderem in Betracht: eine Zertifizierung nach ISO 27001 oder ISO 27017, eine ISO 27001-Zertifizierung auf Basis von IT-Grundschutz, eine Zertifizierung nach anerkannten und geeigneten Branchenstandards oder ein Prüfungsnachweis gemäß SOC / PS 951. Die Zertifizierungs- und Prüfungsverfahren sind von einem anerkannten unabhängigen Dritten durchzuführen. Der Auftragnehmer hat seine Zertifikate oder Prüfungsnachweise, soweit vorhanden, zur Verfügung zu stellen. Die Tätigkeitsberichte des Datenschutzbeauftragten sind ebenfalls geeignete und angemessene Dokumente zum Nachweis der Einhaltung der vereinbarten Schutzmaßnahmen und werden dem Auftraggeber auf Anforderung zur Verfügung gestellt. Das Inspektionsrecht des Auftraggebers aus Ziffer 13.3. bleibt hiervon unberührt.

12.3. Der Auftraggeber ist berechtigt, zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs, regelmäßig nach vorheriger Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit, Inspektionen beim Auftragnehmer zur Prüfung der Einhaltung der datenschutzrechtlichen Bestimmungen durchzuführen. Der Auftragnehmer darf die Inspektion von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der von ihm getroffenen technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen die Beauftragung dieses Prüfers ein Einspruchsrecht.

12.4. Zur Behebung der bei einer Inspektion getroffenen Feststellungen stimmen die Parteien umzusetzende Maßnahmen ab.

12.5. Macht eine Aufsichtsbehörde von Befugnissen nach Art. 58 DSGVO Gebrauch, so informieren sich die Parteien hierüber unverzüglich. Sie unterstützen sich in ihrem jeweiligen Verantwortungsbereich, bei Erfüllung der gegenüber der jeweiligen Aufsichtsbehörde bestehenden Verpflichtungen.

13. Haftung und Schadenersatz

13.1. Macht eine betroffene Person gegenüber einer Partei Schadenersatzansprüche wegen Verstoßes gegen datenschutzrechtliche Bestimmungen geltend, so hat die beanspruchte Partei die andere Partei hierüber unverzüglich zu informieren.

13.2. Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

13.3. Die Parteien unterstützen sich wechselseitig bei der Abwehr von Schadenersatzansprüchen betroffener Personen, es sei denn, dies würde die Rechtsposition der einen Partei im Verhältnis zur anderen Partei oder zur Aufsichtsbehörde gefährden.

14. Kontaktdaten Datenschutz beim Auftragnehmer

Star Finanz-Software Entwicklung und Vertriebs GmbH, Grüner Deich 15, 20097 Hamburg
E-Mail: datenschutz@starfinanz.de

15. Laufzeit

15.1. Der AVV wird auf unbestimmte Zeit geschlossen. Er endet automatisch, ohne dass es dazu einer Kündigung bedarf, mit Beendigung der beauftragten Support-Leistung.

15.2. Der AVV kann mit einer Frist von drei Monaten zum Quartalsende gekündigt werden, wenn gleichzeitig oder zuvor die beauftragte Support-Leistung endet.

16. Schlussbestimmungen

16.1. 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 in Textform zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich in Textform darüber informieren, dass die Verantwortung für die Daten ausschließlich beim Auftraggeber liegt.

16.2. Mündliche Nebenabreden wurden nicht getroffen. Änderungen und Ergänzungen des AVV bedürfen zu ihrer Wirksamkeit der Textform und der ausdrücklichen Bezugnahme auf die AVV. Abweichende mündliche Abreden der Parteien sind unwirksam. Dies gilt auch für Änderungen dieser Klausel.

16.3. Sollte auch nur eine Bestimmung dieser Vereinbarung ganz oder teilweise rechtsunwirksam oder nichtig sein oder werden, bleibt dieser AVV im Übrigen gleichwohl aufrechterhalten und gültig. Anstelle der rechtsunwirksamen oder nichtigen Bestimmung gilt das Gesetz, sofern die hierdurch entstandene Lücke nicht durch ergänzende Vertragsauslegung gemäß §§ 133, 157 BGB geschlossen werden kann. Beide Parteien sind jedoch insoweit verpflichtet, unverzüglich eine rechtswirksame und datenschutzkonforme Vertragsergänzung abzustimmen und zu erstellen.

16.4. Es gilt deutsches Recht.

Technisch-organisatorische Maßnahmen nach Art. 32 DSGVO

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

a) Zutrittskontrolle
Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zutritt zu den Datenverarbeitungsanlagen haben:

- Zutrittskontrollsystem, Ausweisleser (Magnet-/Chipkarte)
- Türsicherungen (elektrische Türöffner, Zahlenschloss, etc.)
- Sicherheitstüren / -fenster
- Schlüsselverwaltung/Dokumentation der Schlüsselvergabe
- Alarmanlage
- Videoüberwachung
- Spezielle Schutzvorkehrungen für die Aufbewahrung von Back-Ups und/oder sonstigen Datenträgern
- Nicht-reversible Vernichtung von Datenträgern

b) Zugangskontrolle
Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zugang zu den Datenverarbeitungssystemen haben.

- Persönlicher und individueller User-Log-In bei Anmeldung am System bzw. Unternehmensnetzwerk
- Autorisierungsprozess für Zugangsberechtigungen
- Begrenzung der befugten Benutzer
- BIOS-Passwörter
- Kennwortverfahren (Angabe von Kennwortparametern hinsichtlich Komplexität und Aktualisierungsintervall)
- Elektronische Dokumentation von Passwörtern und Schutz dieser Dokumentation vor unbefugtem Zugriff
- Protokollierung des Zugangs
- Automatische Sperrung der Clients nach gewissem Zeitablauf ohne Useraktivität (auch passwortgeschützter Bildschirmschoner oder automatische Pausenschaltung)
- Firewall
- sonstiges: Verbindlicher Einsatz von ssh public-key Authentisierung für den Zugang zu Linux-Systemen

c) Zugriffskontrolle
Folgende implementierte Maßnahmen stellen sicher, dass Unbefugte keinen Zugriff auf personenbezogene Daten haben.

- Verwaltung und Dokumentation von differenzierten Berechtigungen
- Abschluss von Verträgen zur Auftragsdatenverarbeitung für die externe Pflege, Wartung und Reparatur von Datenverarbeitungsanlagen, sofern bei der Fernwartung die Verarbeitung von pbD, also der Umgang mit personenbezogenen Daten, Gegenstand der Dienstleistung ist.
- Auswertungen/Protokollierungen von Datenverarbeitungen
- Autorisierungsprozess für Berechtigungen
- Genehmigungsroutinen
- Profile/Rollen
- Verschlüsselung von CD/DVD- ROM, externen Festplatten und/oder Laptops (etwa per Betriebssystem, TrueCrypt, Safe Guard Easy, WinZip, PGP)
- Vier-Augen-Prinzip
- Funktionstrennung „Segregation of Duties“

- Fachkundige Akten- und Datenträgervernichtung gemäß DIN 66399
- Nicht-reversible Löschung von Datenträgern

d) Trennungskontrolle
Folgende Maßnahmen stellen sicher, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden.

- Speicherung der Datensätze in physikalisch getrennten Datenbanken
- Verarbeitung auf getrennten Systemen
- Zugriffsberechtigungen nach funktioneller Zuständigkeit
- Getrennte Datenverarbeitung durch differenzierende Zugriffsregelungen
- Mandantenfähigkeit von IT-Systemen
- Verwendung von Testdaten
- Trennung von Entwicklungs- und Produktionsumgebung

Es erfolgt keine Pseudonymisierung, da dies nicht vereinbart ist.

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

a) Weitergabekontrolle
Es ist sichergestellt, dass personenbezogene Daten bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und überprüft werden kann, welche Personen oder Stellen personenbezogene Daten erhalten haben. Zur Sicherstellung sind folgende Maßnahmen implementiert:

- Verschlüsselung von E-Mail bzw.- E-Mail-Anhängen (z.B. WinZip)
- Verschlüsselung des Speichermediums von Laptops
- Gesicherter File Transfer (z.B. sftp)
- Gesicherter Datentransport (z.B. SSL, ftp, ftps, TLS)
- Verschlüsselung von CD/DVD- ROM, externen Festplatten oder USB-Sticks (z.B. True Crypt, Safe Guard Easy, PGP)
- Gesichertes WLAN
- Fernwartungskonzept (z.B. Verschlüsselung, Ereignisauslösung durch Auftraggeber, Challenge-Response, Rückrufautomatik, Einmal-Passwort)
- „Mobile Device Management-System“
- „Data Loss Prevention (DLP)-System“
- Regelung zum Umgang mit mobilen Speichermedien (z.B. Laptop, USB-Stick, Mobiltelefon)
- Protokollierung von Datenübertragung oder Datentransport
- Getunnelte Datenfernverbindungen (VPN = Virtuelles Privates Netzwerk)

b) Eingabekontrolle
Durch folgende Maßnahmen ist sichergestellt, dass geprüft werden kann, wer personenbezogene Daten zu welcher Zeit in Datenverarbeitungsanlagen verarbeitet hat.

- Zugriffsrechte
- Systemseitige Protokollierungen
- Funktionelle Verantwortlichkeiten, organisatorisch festgelegte Zuständigkeiten
- Mehraugenprinzip

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

Durch folgende Maßnahmen ist sichergestellt, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt und für den Auftraggeber stets verfügbar sind.

- Sicherheitskonzept für Software- und IT-Anwendungen
- Back-Up Verfahren
- Aufbewahrungsprozess für Back-Ups (brandgeschützter Safe, getrennter Brandabschnitt, etc.)
- Gewährleistung der Datenspeicherung im gesicherten Netzwerk
- Bedarfsgerechtes Einspielen von Sicherheits-Updates
- Spiegeln von Festplatten
- Einrichtung einer unterbrechungsfreien Stromversorgung (USV)
- Geeignete Archivierungsräumlichkeiten für Papierdokumente
- Brand- und/oder Löschwasserschutz des Serverraums
- Brand- und/oder Löschwasserschutz der Archivierungsräumlichkeiten
- Klimatisierter Serverraum
- Virenschutz
- Firewall
- Notfallplan
- Erfolgreiche Notfallübungen
- Redundante, örtlich getrennte Datenaufbewahrung (Offsite Storage)
- sonstige: Einsatz von Virtualisierungs-Technologie mit automatischem Fail-Over

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

a) Datenschutz-Management
Folgende Maßnahmen sollen gewährleisten, dass eine den datenschutzrechtlichen Grundanforderungen genügende Organisation vorhanden ist:

- Richtlinien/Anweisungen zur Gewährleistung von technisch-organisatorischen Maßnahmen zur Datensicherheit
- Bestellung eines Datenschutzbeauftragten
- Verpflichtung der Mitarbeiter auf das Datengeheimnis und Bankgeheimnis
- Hinreichende Schulungen der Mitarbeiter in Datenschutzangelegenheiten
- Führen einer Übersicht über Verarbeitungstätigkeiten (Art. 30 DSGVO)
- Durchführung von Datenschutzfolgenabschätzungen, soweit erforderlich (Art. 35 DSGVO)
- sonstige: Durchführung von internen Audits nach dem Standard Sicherer IT-Betrieb (SITB)

b) Incident-Response-Management
Folgende Maßnahmen sollen gewährleisten, dass im Fall von Datenschutzverstößen Meldeprozesse ausgelöst werden:

- Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Betroffenen (Art. 34 DSGVO)

c) Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)
Die Default Einstellungen sind sowohl bei den standardisierten Voreinstellungen von Systemen und Apps als auch bei der Einrichtung der Datenverarbeitungsverfahren zu berücksichtigen. In dieser Phase werden Funktionen und Rechte konkret konfiguriert, wird im Hinblick auf Datenminimierung die Zulässigkeit bzw. Unzulässigkeit bestimmter Eingaben bzw. von Eingabemöglichkeiten (z. B. von Freitexten) festgelegt und über die Verfügbarkeit von Nutzungsfunktionen entschieden (z. B. hinsichtlich des Umfangs der Verarbeitung). Ebenso werden die Art und der Umfang des Personenbezugs bzw. der Anonymisierung (z. B. bei Selektions-, Export- und Auswertungsfunktionen, die festgelegt und voreingestellt oder frei

gestaltbar zur Verfügung gestellt werden können) oder die Verfügbarkeit von bestimmten Verarbeitungsfunktionen, Protokollierungen etc. festgelegt.

- Es werden nur die minimal für den Anwendungszweck erforderlichen Daten abgefragt, zusätzliche optionale Daten werden nicht als Pflichtfelder gekennzeichnet
- Die Eingabe und Übertragung von Daten in Web-Formularen erfolgen grundsätzlich verschlüsselt.
- Es werden Integritätsprüfungen implementiert.

d) Auftragskontrolle
Durch folgende Maßnahmen ist sichergestellt, dass, dass personenbezogene Daten nur entsprechend der Weisungen verarbeitet werden können.

- Vereinbarung zur Auftragsverarbeitung mit Regelungen zu den Rechten und Pflichten des Auftragnehmers und Auftraggebers
- Prozess zur Erteilung und/oder Befolgung von Weisungen
- Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern
- Kontrolle/Überprüfung weisungsgebundener Auftragsdurchführung
- Schulungen/Einweisung aller zugriffsberechtigten Mitarbeiter beim Auftragnehmer
- Verpflichtung der Mitarbeiter auf das Datengeheimnis
- standardisiertes Vertragsmanagement zur Vor- und Nachkontrolle der Dienstleister

Stand April 2026