DATENSCHUTZINFORMATION gem. Art. 13 DSGVO

Im Zuge der Übernahme des uns von Ihnen erteilten Auftrages erhalten wir von Ihnen personenbezogene Daten, die automatisiert verarbeitet werden. Gemäß Art. 13 DSGVO teilen wir Ihnen hierzu folgendes mit:

1. Verantwortliche Stelle ist:
   zeitsprung GmbH
   Wilhelm-Becker-Straße 11a
   75179 Pforzheim
   Telefon: 07231 / 166093-0
   support@zeitsprung.digital

2. Datenschutzbeauftragter ist:
   Herr Andreas Lingenfelser
   Telefon: 07231 / 166093-2
   datenschutz@zeitsprung.digital

3. Zwecke und Rechtsgrundlagen der Verarbeitung:
   Ihre Daten werden zum Zwecke der Durchführung des uns von Ihnen erteilten Auftrags, z. Bsp. Nutzung eines zeitsprung-Lizenzproduktes, damit verbundenen Testzugängen oder Kontaktaufnahmen, oder auch zum Zweck des Bewerbungsprozesses, verarbeitet. Die Rechtsgrundlage dafür ist die Erfüllung des mit Ihnen bestehenden Vertrages (Art. 6 Abs. 1 lit.b DSGVO) oder einer entsprechenden Anbahnung zur Zusammenarbeit.

   Soweit Sie uns eine Einwilligung zur Verarbeitung personenbezogener Daten für bestimmte Zwecke erteilt haben, ist die Rechtmäßigkeit der Verarbeitung auf Basis Ihrer Einwilligung gegeben (Art. 6 Abs. 1 lit. a DSGVO). Eine erteilte Einwilligung kann jederzeit widerrufen werden. Bitte beachten Sie aber, dass der Widerruf erst für die Zukunft wirkt. Verarbeitungen, die vor dem Widerruf erfolgt sind, sind davon also nicht betroffen.

   Soweit wir gesetzliche Vorgaben (z. Bsp. Aufbewahrungspflichten nach HGB und AO) erfüllen müssen, ist die Rechtsgrundlage Art. 6 Abs. 1 lit. c DSGVO. Im Einzelfall kann sich die Rechtmäßigkeit der Verarbeitung zudem aus einer Interessenabwägung (Art. 6 Abs. 1 lit. f DSGVO), zum Beispiel bei Direktwerbung, ergeben.

4. Empfänger der Daten:

   Innerhalb unseres Unternehmens erhalten Ihre Daten diejenigen Mitarbeiter, die Ihren Auftrag bearbeiten. Weitere Empfänger sind von uns eingesetzte Auftragsverarbeiter (z. Bsp. Rechenzentren).

5. Übermittlung an ein Drittland:

   Eine Übermittlung Ihrer Daten an Drittländer findet nicht statt, es sei denn, Ihr Auftrag beinhaltet dies oder es besteht eine gesetzliche Verpflichtung hierzu.

6. Dauer der Speicherung:

   Wir verarbeiten und speichern Ihre personenbezogenen Daten für die Dauer unserer Geschäftsbeziehung mit Ihnen. Darüber hinaus unterliegen wir verschiedenen Aufbewahrungs- und Dokumentationspflichten, die sich aus HGB und AO ergeben.
   Die dort vorgegebenen Fristen betragen sechs bzw. zehn Jahre. Schließlich richtet sich die Speicherdauer auch nach den gesetzlichen Verjährungsfristen, §195ff. BGB, die in der Regel drei oder zehn Jahre betragen.

7. Datenschutzrechte:

   Als betroffene Person haben Sie uns gegenüber ein Recht auf Auskunft nach Art. 15 DSGVO, ein Recht auf Berichtigung nach Art. 16 DSGVO, ein Recht auf Löschung nach Art.17 DSGVO, ein Recht auf Einschränkung der Verarbeitung nach Art. 18 DSGVO sowie ein Recht auf Datenübertragbarkeit nach Art. 20 DSGVO.

   Beim Auskunftsrecht und beim Löschungsrecht gelten die Einschränkungen der §§ 34 und 35 BDSG. Darüber hinaus besteht ein Beschwerderecht bei einer Datenschutzaufsichtsbehörde (Art. 77 DSGVO i. V. m. § 19 BDSG).

8. Pflicht zur Bereitstellung von Daten:

   Im Rahmen des bestehenden oder zukünftigen Vertragsverhältnisses müssen Sie nur diejenigen personenbezogenen Daten bereitstellen, die für die Durchführung Ihres Auftrages erforderlich sind oder zu deren Erhebung wir gesetzlich verpflichtet sind.

9. Automatisierte Entscheidungsfindung: findet nicht statt.

10. Verarbeitung zu einem anderen Zweck:

    Soweit eine Verarbeitung Ihrer Daten für einen anderen Zweck, als den, für den sie erhoben wurden, beabsichtigt ist, werden wir Ihnen dies rechtzeitig mitteilen und Ihnen weitere Informationen hierzu zur Verfügung stellen.

Vorstehende Informationen habe ich erhalten und zur Kenntnis genommen:

_____

Ort / Datum / Unterschrift

INFORMATION ÜBER IHR WIDERSPRUCHSRECHT NACH ART. 21 DSGVO

Sie haben das Recht, aus Gründen, die sich aus Ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung Sie betreffender personenbezogener Daten, die aufgrund von Art. 6 Abs. 1 lit. e DSGVO (Datenverarbeitung im öffentlichen Interesse) oder Art. 6 Abs. 1 lit. f DSGVO (Datenverarbeitung aufgrund einer Interessenabwägung) erfolgt, Widerspruch einzulegen.

Legen Sie Widerspruch ein, werden wir Ihre personenbezogenen Daten nicht mehr verarbeiten, es sei denn, wir können zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die Ihre Interessen, Rechte und Freiheiten überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Sofern wir Ihre Daten zum Zwecke der Direktwerbung verarbeiten, haben Sie das Recht, jederzeit Widerspruch gegen die Verarbeitung Sie betreffender personenbezogener Daten zum Zwecke derartiger Werbung einzulegen. Widersprechen Sie der Verarbeitung für Zwecke der Direktwerbung, so werden wir Ihre personenbezogenen Daten nicht mehr für diese Zwecke verarbeiten.

Der Widerspruch kann formfrei erfolgen und ist zu richten an:

zeitsprung GmbH
Datenschutzbeauftragter
Wilhelm-Becker-Straße 11a
75179 Pforzheim

Vorstehende Informationen habe ich erhalten und zur Kenntnis genommen:

_____

Ort / Datum / Unterschrift

Dienstleisterverzeichnis

Subunternehmer der zeitsprung GmbH im Sinne der Auftragsverarbeitungs-Vereinbarung (**Stand 10.07.2025**) sind:

Subunternehmer	**Funktion**
NetPlans GmbH Eisenstockstr. 12 76275 Ettlingen Tel. 07243 37340 E-Mail info@netplans.de	Support und Implementierung, System-Housing und Service-Management Verarbeitung ausschließlich innerhalb Deutschland
TelemaxX Telekommunikation GmbH Amalienbadstr. 41 / Bau 61 76227 Karlsruhe Tel. 0721 13088-0 E-Mail info@telemaxx.de	Betrieb eines Rechenzentrums Verarbeitung ausschließlich innerhalb Deutschland
1&1 Internet SE Eigendorfer Str. 57 56410 Montabaur Tel. 0721 9600 E-Mail info@1und1.de	Betrieb der Internetdomains, Betrieb der E-Mailinfrastruktur Verarbeitung ausschließlich Deutschland
softfair GmbH (Trixi) Albert-Einstein-Ring 15 22761 Hamburg Tel. 040 609 434-00 E-Mail info@softfair.de	Tarifierung und Beantragung von KFZ-Versicherungsverträgen Verarbeitung ausschließlich innerhalb Deutschland
letterei.de Postdienste GmbH Frankfurter Str. 74 64521 Groß – Gerau Tel. 06152 99 8 98 – 0 E-Mail: info@letterei.de	Versand von Postbriefen Verarbeitung ausschließlich innerhalb Deutschland
Elasticsearch B.V. Keizersgracht 281, Amsterdam, Noord-Holland, 1016ED Internet: www.elastic.co	Betrieb einer internen Protokollierungsplattform, Analysewerkzeug für Logdateien Verarbeitung ausschließlich innerhalb der EU (Region Frankfurt)
Amazon Web Services EMEA SARL 38 Avenue John F. Kennedy L-1855 Luxembourg Internet: www.aws.amazon.com	Bereitstellung von Cloud- und Hosting-Dienstleistungen Verarbeitung ausschließlich innerhalb der EU (Region Frankfurt)
Microsoft Operations Ltd. One Microsoft Place, South County Business Park, Carmanhall And Leopardstown, Dublin, D18 P521, Irland Internet: www.microsoft.com	Bereitstellung und Betrieb von Cloud- und Hosting-Dienstleistungen Verarbeitung ausschließlich innerhalb der EU (Region Frankfurt)
Hornet Security GmbH Am Listholze 78 30177 Hannover als Unterauftragnehmer der QUANTUM Holding GmbH Beethovenstr. 43 77767 Appenweier www.qdna.it	Bereitstellung und Betrieb von Sicherheitslösungen und Cloudspeicher-Dienstleistungen Verarbeitung ausschließlich innerhalb Deutschlands (Region Düsseldorf)

Atlassian. Pty Ltd Level 6, 341 George Street Sydney NSW 2000 Australien	Bereitstellung und Betrieb von Cloud- und Hosting-Dienstleistungen

Technisch-organisatorische Maßnahmen nach Art. 32 DSGVO

Unternehmen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der EU-DSGVO zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Das Unternehmen erfüllt diesen Anspruch durch folgende Maßnahmen (**Stand 10.07.2025**):

1. Zutrittskontrolle

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

☒ Zutrittskontrollsystem, Ausweisleser (Magnet- / Chipkarte)	☒ Mitarbeiter- und Berechtigungsausweise (nur im Rechenzentrum – nicht im Büro)
☒ Türsicherungen (elektrische Türöffner, Zylinderschloss)	☒ Sperrbereiche (nur im Rechenzentrum – nicht im Büro)
☒ Manuelles Schließsystem und Sicherheitsschlösser, Türen mit Knauf Außenseite	☒ separate Schlösser für DV-Schränke
☒ Gitter vor Türen / Fenstern (nur im Rechenzentrum – nicht im Büro)	☒ Spezielle Schutzvorkehrungen für die Aufbewahrung von Back-ups und / oder sonstigen Datenträgern
☐ Zaunanlagen	☐ Videoüberwachung im Eingangsbereich
☒ Schlüsselverwaltung / Dokumentation der Schlüsselvergabe	☒ Besucherregelung (Abholung am Empfang, Dokumentation von Besuchern)
☒ Empfang	☒ Alarmanlage mit Wachschutzaufschaltung
☒ Sorgfalt bei Auswahl der Reinigungsdienste	☒ Sorgfalt bei Auswahl des Wachpersonals

2. Zugangskontrolle

Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zugang zu den Datenverarbeitungssystemen haben:

☒ Persönlicher und individueller User-Log-In bei Anmeldung am System	☒ Begrenzung der befugten Benutzer

☒ Autorisierungsprozess für Zugangsberechtigungen	☒ Single Sign-on
☐ Boot-Passwörter	☒ Kennwortverfahren/ Zentrale Passwortvergabe, Richtlinie „Sicheres Passwort“
☐ BIOS-Passwörter	☒ Elektronische Dokumentation von Passwörtern und Schutz dieser Dokumentation vor unbefugtem Zugriff
☐ Personalisierte Chipkarten	☒ Protokollierung des Zugangs
☒ Zusätzlicher System-Log-In für bestimmte Anwendungen	☒ Automatisierte Sperrung der Clients nach gewissem Zeitablauf ohne Useraktivität
☒ Firewall	☒ Webapplication-Firewall
☒ Login mit Benutzername + Passwort	☒ Mobile Device Management/ Mobile Device Policy
☒ Login mit biometrischen Daten	☒ Einsatz VPN bei Remote-Zugriffen
☒ Anti-Viren-Software Server	☒ Verschlüsselung von Datenträgern
☒ Anti-Virus-Software Clients	☐ Verschlüsselung Smartphones
☒ Intrusion Detection Systeme	☒ Richtlinien zu „Clean desk“, „Manuelle Desktopsperre“, Allg. Richtlinie Datenschutz & Sicherheit, Richtlinie „Sicheres Passwort“, „Löschen / Vernichten“
☒ Endpoint-Security-Systeme (z.B. Schutz von externen Schnittstellen (USB))	

3. Zugriffskontrolle

Folgende implementierte Maßnahmen stellen sicher, dass Unbefugte keinen Zugriff auf personenbezogene Daten haben:

☒ Verwaltung und Dokumentation von differenzierten Berechtigungen	☒ Mobile Device Management System
☒ Abschluss von Verträgen zur Auftragsdaten-verarbeitung für die externe Pflege, Wartung und Reparatur von Datenverarbeitungsanlagen, sofern bei der Fernwartung die Verarbeitung von personenbezogenen Daten, also der Umgang mit personenbezogenen Daten Gegenstand der Dienstleistung ist	☒ Vier-Augen-Prinzip
☒ Auswertung / Protokollierung von Datenverarbeitungen	☒ Funktionstrennung / Segregation of Duties
☒ Autorisierungsprozess für Berechtigungen	☒ Fachkundige Akten- und Datenträgervernichtung nach DIN 66399

☒ Genehmigungsrichtlinien und Freigabeprozess	☒ Nicht reversible Löschung von Datenträgern
☒ Profile / Rollen	☒ Sichtschutzfolien für mobile Datenverarbeitungssysteme
☒ Verschlüsselung von externen Datenträgern und Laptops	☒ Datenschutztresor
☒ Maßnahmen zur Verhinderung unbefugten Überspielens von Daten auf extern verwendbare Datenträger	☒ Minimale Anzahl an Administratoren und Verwaltung der Benutzerrechte ausschließlich durch Administratoren
☒ Einsatz Berechtigungskonzepte	

4. Trennungskontrolle

Folgende Maßnahmen stellen sicher, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden:

☐ Speicherung der Datensätze in physikalisch getrennten Datenbanken	☒ Getrennte Datenverarbeitung durch differenzierende Zugriffsregelungen
☒ Speicherung der Datensätze in zweckgebunden getrennten Datenbanken	☒ Mandantenfähigkeit von IT-Systemen
☒ Speicherung der Datensätze durch Mandantenkennzeichen	☒ Verwendung von Testdaten
☒ Verarbeitung auf getrennten Systemen	☒ Trennung von Entwicklungs- und Produktionsumgebung
☒ Zugriffsberechtigungen nach funktioneller Zuständigkeit	☐ Daten mit Zweckattributen versehen

5. Pseudonymisierung

Die Verarbeitung personenbezogener Daten erfolgt 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.

☒ *Eine derartige Verarbeitung ist für den bestehenden Vertrag aktuell nicht vorgesehen.*

☐ *Eine derartige Verarbeitung ist für den bestehenden Vertrag erforderlich.*

6. Weitergabekontrolle

Es wird 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 dessen sind folgende Maßnahmen implementiert:

☒ Verschlüsselung von Emails bzw. Email-Anhängen	☒ Fernwartungskonzept mit Verschlüsselung und Einmal-Passwort
☒ Verschlüsselung des Speichermediums von Laptops	☒ Mobile Device Management System
☒ Gesicherter Filetransfer per SFTP	☒ Data Loss Prevention System
☒ Gesicherter Datentransport per SSL (HTTPS)	☒ Regelung zum Umgang mit mobilen Speichermedien
☒ Verschlüsselung von externen Festplatten oder USB-Sticks	☒ Protokollierung von Datenübertragung und Datentransport
☒ Physikalische Transportsicherung	☒ Protokollierung von lesenden Zugriffen
☐ Verpackungs- und Versandvorschriften	☒ Protokollierung des Änderns oder Entfernens von Daten (keine Protokollierung der Kopiervorgänge)
☒ Elektronische Signatur	☒ Getunnelte Datenfernverbindungen (VPN= Virtuelles privates Netzwerk)
☒ Gesichertes WLAN	

7. Eingabekontrolle

Durch folgende Maßnahmen wird sichergestellt, dass geprüft werden kann, wer personenbezogene Daten zu welcher Zeit in Datenverarbeitungsanlagen verarbeitet hat:

☒ Zugriffsrechte	☒ Mehraugenprinzip
☒ Systemseitige Protokollierungen	☒ Data Loss Prevention System
☒ Dokumenten Management System (DMS) mit Änderungshistorie	☒ Datenlöschrichtlinie
☒ Sicherheits- / Protokollierungssoftware	☒ Separatisierte Berechtigungen für Hinzufügen, Ändern, Löschen, Einsehen
☒ Funktionelle Verantwortlichkeiten, organisatorisch festgelegte Zuständigkeiten	

8. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit.b. DSGVO)

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	☒ Brand- und / oder Löschwasserschutz des Serverraums im Rechenzentrum
☒ Back-up-Verfahren	☐ Brand- und / oder Löschwasserschutz der Archivierungsmöglichkeiten
☒ Aufbewahrungsprozess für Back-ups (brandgeschützter Safe)	☒ Klimatisierter Serverraum
☒ Gewährleistung der Datenspeicherung im gesicherten Netzwerk	☒ Virenschutz
☒ Bedarfsgerechtes Einspielen von Sicherheits-Updates	☒ Firewall
☒ Spiegeln von Festplatten an Servern	☒ Notfallplan
☒ Einrichtung einer unterbrechungsfreien Stromversorgung (USV)	☒ Erfolgreiche Notfallübungen
☒ Geeignete Archivierungsmöglichkeiten für Papierdokumente	☒ Redundante, örtlich getrennte Datenaufbewahrung
☒ Feuer- und Rauchmeldeanlagen	☒ Kontrolle des Sicherungsvorgangs
☒ Feuerlöscher Serverraum im Bürobetrieb ☒ Feuerlöscher Serverraum im Rechenzentrum	☒ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
☐ Serverraumüberwachung: Temperatur	☒ Regelmäßige Tests zur Datenwiederherstellung
☒ Schutzsteckdosenleisten Serverraum	☒ Getrennte Partitionen für Betriebs-systeme und Daten
☐ Alarmmeldung bei unberechtigtem Zutritt zu Serverraum	☒ Keine sanitären Anschlüsse im oder oberhalb des Serverraums
☒ Videoüberwachung Serverraum im Bürobetrieb ☒ Videoüberwachung Serverraum im Rechenzentrum	☒ Dauerhafte Überwachung der Verfügbarkeit geschäftskritischer Server von verschiedenen Standorten (Außenverfügbarkeit/ Dienstverfügbarkeit)

9. Datenschutzmanagement

Folgende Maßnahmen sollen gewährleisten, dass eine den datenschutzrechtlichen Grundanforderungen genügende Organisation vorhanden ist:

☒ Datenschutzleitbild des Auftragnehmers	☒ Hinreichende Schulung der Mitarbeiter in Datenschutzangelegenheiten

☒ Datenschutzrichtlinie des Auftragnehmers	☒ Führen einer Übersicht über Verarbeitungstätigkeiten (Art. 30 DSGVO)
☒ Richtlinien / Anweisungen zur Gewährleistung von technisch-organisatorischen Maßnahmen zur Datensicherheit	☒ Durchführung von Datenschutzfolgenabschätzungen
☒ Bestellung eines Datenschutzbeauftragten	☒ Externe Prüfung / Auditierung der Informationssicherheit
☒ Verpflichtung der Mitarbeiter auf das Datengeheimnis	☒ Regelmäßige Überprüfung des Datenschutzmanagements

10. Incident-Response-Management

Folgende Maßnahmen sollen gewährleisten, dass im Fall von Datenschutzverletzungen Meldeprozesse ausgelöst werden:

☒ *Meldeprozess nach Art. 4 Ziff. 12 DSGVO gegenüber Aufsichtsbehörden (Art. 33 DSGVO)*

☒ *Meldeprozess nach Art. 4 Ziff. 12 DSGVO gegenüber Betroffenen (Art. 34 DSGVO)*

11. Datenschutzfreundliche Voreinstellungen

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. Eingabemöglichkeiten festgelegt und über die Verfügbarkeit von Nutzungsfunktionen entschieden. Ebenso werden die Art und der Umfang des Personenbezuges bzw. der Anonymisierung oder die Verfügbarkeit von bestimmten Verarbeitungsfunktionen, Protokollierungen etc. festgelegt.

☒ Kennzeichnung der erforderlichen Eingabefelder in Onlineformularen (Pflichtfelder)	☒ Benachrichtigungen nur kurzzeitig anzeigen vorbelegt
☒ Keine Vorbelegung zur Teilnahme an Newslettern oder Werbeansprachen	☒ Sichtzugriff für Benutzerkonten bei der Neuanlage auf eigene Daten des Benutzers vorbelegt
☒ Option um verschlüsselte Verbindungen auf Kundenportalen zu erzwingen	☒ Optionen für Informationsweiterleitungen per E-Mail im Auslieferungszustand deaktiviert
☒ Option für sichere Kennwörter zu erzwingen	☒ Automatische Löschung von Informationen nach Abholung von Daten im Auslieferungszustand deaktiviert

☒ Opt-In Verfahren für die Freischaltung von Zugängen erzwungen	☒ Zugriff auf erweiterte Funktionalitäten im Auslieferungszustand deaktiviert
☒ Benutzerrechte-Vererbung auf angelegte Benutzer des anlegenden Profils (aktive Rechteweitergabebegrenzung)	☐ Anonymisierte Anmeldung zu einem Newsletter
☒ Bestätigungsverfahren zur Kennwortänderung (Kennwort vergessen)	

12. Auftragskontrolle

Durch folgende Maßnahmen wird sichergestellt, dass personenbezogene Daten nur entsprechend der Weisung verarbeitet werden:

☒ Vereinbarung zur Auftragsverarbeitung	☒ formalisiertes Auftragsmanagement
☒ Prozess zur Erteilung und / oder Befolgung von Weisungen	☒ dokumentiertes Verfahren zur Auswahl von Dienstleistern
☒ Bestimmung von Ansprechpartnern und / oder verantwortlichen Mitarbeitern	☒ standardisiertes Vertragsmanagement zur Vor- und Nachkontrolle von Dienstleistern
☒ Kontrolle / Überprüfung weisungsgebundener Auftragsdurchführung	☒ Vorherige Prüfung der vom Auftrag-Nehmer getroffenen Sicherheitsmaß-nahmen und deren Dokumentation
☒ Schulung / Einweisung aller zugriffsberechtigten Mitarbeiter beim Auftragnehmer	☒ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicher-heit
☐ Unabhängige Auditierung der Weisungsgebundenheit	☒ Verpflichtung zur Bestellung eines Daten-schutzbeauftragten durch den Auftrag-nehmer bei Vorliegen Bestellpflicht
☒ Verpflichtung der Mitarbeiter auf das Datengeheimnis	☒ Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus