

Vereinbarung über die Verarbeitung von Daten im Auftrag

zwischen der jeweils beitretenen regionalen Industrie- und Handelskammer (IHK) –

- Verantwortlicher, nachfolgend „...“ oder „Auftraggeber“-

und [Plattformanbieter]

- Auftragsverarbeiter, nachfolgend "...“ oder „Auftragnehmer“-

Präambel

Der Auftraggeber hat am **xx.xx.201x** den Auftragnehmer mit (*Bezeichnung des Vertragsgegenstands*) auf Grundlage des von der DIHK verhandelten Rahmenvertrags und seiner Beitrittserklärung mit der Bereitstellung und dem Betrieb der digitalen Prüfungsplattform beauftragt (vgl. Leistungsbeschreibung/Anforderungskatalog) beauftragt. Auf die Vertragsinhalte wird Bezug genommen. Diese Vereinbarung legt die datenschutzrechtlichen Verpflichtungen der Vertragsparteien im Rahmen der Auftragsverarbeitung fest. Jede regionale IHK schließt diese Vereinbarung als alleiniger Verantwortlicher (Art. 4 Nr. 7 DSGVO) unmittelbar und inhaltlich unverändert mit dem Auftragnehmer ab.

§ 1 Gegenstand und Dauer des Auftrags (Art. 28 Abs. 3)

- (1) Der Auftragnehmer verpflichtet sich, im Auftrag des Auftraggebers die in § 2 spezifizierten personenbezogenen Daten zu den im Vertrag/der Leistungsbeschreibung dargestellten Zwecken zu verarbeiten.
- (2) Bestimmt der Auftragnehmer die Zwecke und Mittel der Verarbeitung unter Verstoß gegen die DSGVO und diese Vereinbarung, ist er bezüglich der in dieser Vereinbarung geregelten Verarbeitung selbst Verantwortlicher und haftet entsprechend gemäß Art. 82 DSGVO.
- (3) Die Vereinbarung beginnt mit dem Beitritt und endet mit Beendigung des zugrunde liegenden Vertrags. Das Recht zur Kündigung aus wichtigem Grund bleibt unberührt.
- (4) Der Auftraggeber kann die Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die Bestimmungen der DSGVO, des Bundesdatenschutzgesetzes bzw. des Landesdatenschutzgesetzes und weiterer datenschutzrechtlicher Vorschriften oder dieser Vereinbarung vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollen des Auftraggebers oder des Landesdatenschutzbeauftragten/Bundesdatenschutzbeauftragten vertragswidrig verweigert.
Widerspricht der Auftraggeber dem Einsatz eines Unterauftragsverarbeiters aus wichtigem datenschutzrechtlichem Grund (§ 6) und kann der Auftragnehmer den Widerspruch nicht durch technische Maßnahmen (z. B. Mandantenausschluss)

heilen, steht dem Auftraggeber ein sofortiges, kostenfreies Sonderkündigungsrecht für die Plattformnutzung zu.

§ 2 Umfang, Art und Zweck der Datenverarbeitung (Art. 28 Abs. 3)

- (1) Gegenstand der Verarbeitung sind folgende Datenarten/-kategorien:
- Stammdaten (Name, Geburtsdatum, Prüflingsnummer, Kammerzugehörigkeit);
 - Kontaktdaten (E-Mail, Mobilfunknummer, ausschließlich zur 2-Faktor-Authentifizierung privilegierter Nutzer);
 - Zugangs- und Authentifizierungsdaten;
 - Organisations- und Prüfungsmetadaten (Termin, Ort, Raum-/Aufsichtszuordnung, gewährte Schreibzeitverlängerung);
 - Prüfungsleistungs-, Bewertungs- und Ergebnisdaten sowie Klickpfad-/Revisionsprotokolle;
 - besondere Kategorien personenbezogener Daten (Art. 9 Abs. 1 DSGVO): abstrakte Umsetzungsparameter des bewilligten Nachteilsausgleichs. Diagnosen, Attest-Inhalte, Grad der Behinderung und medizinische Nachweise werden auf der Plattform nicht verarbeitet

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen: Prüflinge (einschließlich Minderjähriger und Menschen mit Behinderung), Prüferinnen und Prüfer, Prüfungsaufsichten, IHK-Mitarbeitende.

- (2) Der Auftragnehmer verarbeitet die personenbezogenen Daten nach § 1 Abs. 1 ausschließlich im Rahmen des Auftrages gemäß § 1 und nach dokumentierten Weisungen des Auftraggebers. Der Auftragnehmer verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen Zwecke. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherungskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind.
- (3) Der Auftragnehmer führt innerhalb dieses Auftrags alle technischen Maßnahmen für die Sicherstellung des Vertragszwecks sowie die Sicherheit und/oder Verarbeitungen der Daten (z. B. Duplizieren von Beständen für die Verlustsicherung, Anlegen von Log-Files etc.) durch, soweit sie nicht zu inhaltlichen Änderungen der Daten führen und sie zur Erfüllung des Auftrags erforderlich sind.
- (4) Die Verarbeitung der Daten auch durch Unterauftragnehmer findet ausschließlich in zertifizierten Rechenzentren (mindestens ISO 27001 oder gleichwertig) innerhalb der EU bzw. des EWR statt; dies gilt für die gesamte Unterauftragsverarbeiterkette. Sämtliche Support-, Wartungs-, Administrations- und Remote-Zugriffe auf Plattform und Hosting-Infrastruktur erfolgen physisch aus der EU/dem EWR; ein Follow-the-Sun-Support aus Drittländern ist ausgeschlossen. Jeder Zugriff aus einem Drittland gilt als Übermittlung i. S. d. Art. 44 DSGVO. Eine Verlagerung in ein Drittland bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers und ist nur bei Vorliegen der Voraussetzungen des Kapitels V DSGVO (Art. 44 ff.) einschließlich der nach der Rechtsprechung erforderlichen zusätzlichen Maßnahmen zulässig. Bei Nutzung einer Public-Cloud-Infrastruktur mit Drittlandsbezug legt der Auftragnehmer vor Verarbeitungsbeginn ein lückenloses Transfer Impact Assessment (TIA) vor.

§ 3 Technische und organisatorische Maßnahmen/Sicherheit der Verarbeitung (Art. 28 Abs. 1, Abs. 3 c, Art. 32)

- (1) Der Auftragnehmer trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO; sie sind in **Anlage 1** gesondert festgeschrieben und Vertragsbestandteil. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen

bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten. Die Angemessenheit der Maßnahmen für die Risiken der verarbeiteten Daten ist vom Auftragnehmer als Fachkundigem für die von ihm bereitgestellte Plattform sicherzustellen; der Auftraggeber genehmigt die dargelegten Maßnahmen. Das vereinbarte Schutzniveau darf nachträglich nicht unterschritten werden.

- (2) Der Auftragnehmer setzt ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der Maßnahmen ein.
- (3) Der Auftragnehmer passt die Maßnahmen dem Stand der Technik an, soweit dies erforderlich und zumutbar ist. Alternative adäquate Maßnahmen sind zulässig, sofern das vereinbarte Sicherheitsniveau nicht unterschritten wird; wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber vorab mitzuteilen.
- (4) Anlage 1 bildet insbesondere ab: strikte logische Mandantentrennung/Tenant-aware Design und kryptografische Schematrennung je Mandanten-ID (AK APP-01, INF-08), MFA für privilegierte Rollen (AK APP-03), Sitzungs-Timeout (APP-04), pseudonymisierte Korrekturmasks und gekapselte Identitätszuordnung (APP-05/06), gesondert verschlüsselter Datenbereich mit eigenem Schlüsselmaterial für Nachteilsausgleichsparameter (APP-16), Verschlüsselung data at rest (AES-256) und in transit (TLS 1.3/mTLS), bei Public-Cloud-Nutzung HYOK/BYOK mit Schlüsselhoheit außerhalb des Cloud-Anbieters (INF-04) sowie ein schreibgeschützter SIEM-Logserver mit 7-Tage-Löschung der IP-Adressen (INF-11). Die Maßnahmen des Auftragnehmers und seiner Unterauftragnehmer entsprechen dem Stand der Technik.

§ 4 Berichtigung, Einschränkung der Verarbeitung und Löschung von Daten, Auskunft über Daten (Art. 28 Abs. 3)

Der Auftragnehmer hat nur nach dokumentierter Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken. Die Plattform stellt hierfür Sperr-Flags bereit, mit denen Daten – insbesondere bei schwebenden Widerspruchsverfahren – manuell von automatisierten Löschfristen ausgenommen werden können (AK APP-15).

§ 5 Pflichten des Auftragnehmers (Art. 28 Abs. 3 h, Art. 32)

- (1) Der Auftragnehmer hat die Beachtung der datenschutzrechtlichen Vorschriften im Hinblick auf das Auftragsverhältnis sicherzustellen. Stellt der Auftragnehmer Unregelmäßigkeiten fest, wird er unverzüglich den Auftraggeber informieren. Der Auftragnehmer sichert zu, die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt zu trennen.
- (2) Der Auftragnehmer verpflichtet sich, bei der Verarbeitung personenbezogener Daten des Auftraggebers die Vertraulichkeit sowie etwaige berufliche Verschwiegenheitsverpflichtungen (insbesondere die durch gesetzliche und dienstrechtliche Verschwiegenheitspflichten geschützten) zu wahren und dem Auftraggeber nachzuweisen. Er hat bei der Verarbeitung ausschließlich Beschäftigte einzusetzen, die entsprechend verpflichtet und geschult sind. Er hat insbesondere mit der gebotenen Sorgfalt darauf hinzuwirken, dass alle Personen, die von ihm mit der Bearbeitung oder Erfüllung dieses Vertrages betraut sind, sorgfältig ausgewählt werden, die gesetzlichen Bestimmungen über den Datenschutz beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht unbefugt an Dritte weitergeben oder sonst verwerten.

- (3) Der Auftragnehmer hat einen betrieblichen Datenschutzbeauftragten bestellt und teilt dessen jeweils aktuelle Kontaktdaten leicht zugänglich mit; ein Wechsel ist unverzüglich mitzuteilen.
- (4) Der Auftragnehmer verpflichtet sich, ein Verarbeitungsverzeichnis gemäß Art. 30 Abs. 2 DSGVO zu führen.
- (5) Der Auftragnehmer gewährt der zuständigen Aufsichtsbehörde Zugang zu den Arbeitsräumen und unterwirft sich deren Kontrolle.
- (6) Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie den Vertragsgegenstand betreffen.
- (7) Wenden sich betroffene Personen an den Auftragnehmer, verweist er sie unverzüglich an den Auftraggeber. Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung der Betroffenenrechte im erforderlichen Umfang.
- (8) Der Auftragnehmer unterstützt den Auftraggeber bei den Pflichten aus Art. 32–36 DSGVO, insbesondere bei Meldungen nach Art. 33/34, bei der Erstellung und Aktualisierung der Muster-Datenschutz-Folgenabschätzung durch Bereitstellung aller erforderlichen technischen Dokumentationen, Architekturdiagramme, Datenflussbeschreibungen und Risikoanalysen – kostenfrei (AK GOV-04; DSK Ziff. 6.2) sowie bei vorherigen Konsultationen. Geplante funktionale Änderungen legt der Auftragnehmer vorab vor; eine Freischaltung für einen IHK-Mandanten erfolgt erst nach lokaler Übernahme der aktualisierten Muster-DSFA.

§ 6 Unterauftragsverhältnisse (Art. 28 Abs. 2, Abs. 3 d, Abs. 4)

- (1) Der Beauftragung der in Anlage 2 namentlich benannten Unterauftragnehmer stimmt der Auftraggeber mit Unterzeichnung zu (allgemeine schriftliche Genehmigung, Art. 28 Abs. 2 DSGVO).
- (2) Der Abschluss zukünftiger Unterauftragsverhältnisse bedarf der vorherigen Zustimmung des Auftraggebers. Die Zustimmung darf nur aus wichtigen datenschutzrechtlichen Gründen verweigert werden.
- (3) Jede geplante Einbindung, Änderung oder Ersetzung eines Unterauftragnehmers zeigt der Auftragnehmer mindestens sechs (6) Wochen vor dem geplanten Einsatz schriftlich [] an. Der Auftraggeber kann dem Einsatz innerhalb der Anzeigefrist aus wichtigem datenschutzrechtlichem Grund widersprechen. Kann der Auftragnehmer den Widerspruch nicht durch technische Maßnahmen (z. B. Mandantenausschluss) heilen, gilt das Sonderkündigungsrecht nach § 1 (AK GOV-03).
- (4) Der Auftragnehmer erlegt dem Unterauftragnehmer dieselben Datenschutzpflichten auf, die ihn selbst treffen (Art. 28 Abs. 4 DSGVO), und stellt sicher, dass der Auftraggeber und die zuständige Aufsichtsbehörde ihre Kontrollrechte auch unmittelbar gegenüber dem Unterauftragnehmer ausüben können. Erbringt der Unterauftragnehmer außerhalb EU/EWR – hier ausgeschlossen (§ 2) –, gilt § 2 entsprechend.
- (5) Der Auftragnehmer haftet gegenüber dem Auftraggeber vollumfänglich für Datenschutzverstöße seiner Unterauftragnehmer.

§ 7 Kontrollrechte des Auftraggebers (Art. 28 Abs. 3 h)

- (1) Der Auftraggeber ist berechtigt, sich – auch durch beauftragte Prüfer – von der Einhaltung dieser Vereinbarung, insbesondere der TOM, zu überzeugen. Der Nachweis kann vorrangig durch aktuelle Testate, Zertifikate (z. B. ISO 27001) oder Berichte unabhängiger Instanzen geführt werden; Vor-Ort-Kontrollen bleiben möglich, soweit sie gesetzlich erforderlich sind oder Zertifikate/Testate nicht ausreichen (AK GOV-05).
- (2) Zentralisiertes Audit-Verfahren: Der Auftragnehmer duldet und sichert vertraglich zu, dass die IHK-Organisation – vertreten durch den hierzu von den IHKs bevollmächtigten Lenkungskreis – einmal jährlich ein gemeinsames, umfassendes Datenschutz- und Sicherheitsaudit beim Auftragnehmer und seinen Rechenzentren durch einen unabhängigen, zertifizierten Prüfer durchführen lässt. Der Bericht wird allen IHKs zur Verfügung gestellt. Das individuelle Kontrollrecht der einzelnen IHK nach Abs. 1 bleibt unberührt.
- (3) Zusätzlich ist die Plattform (Ebene 2 und 3) alle zwei Jahre sowie vor jedem Major-Release durch einen unabhängigen, zertifizierten IT-Sicherheitsdienstleister einem Penetrationstest zu unterziehen; die Ergebnisse werden dem Auftraggeber auf Anfrage vorgelegt (DSK Ziff. 15.2).

§ 8 Mitteilung bei Verstößen (Art. 33 Abs. 2)

- (1) Der Auftragnehmer meldet dem Auftraggeber unverzüglich – bereits bei jeder Möglichkeit eines unbefugten Zugriffs oder eines sonstigen Verstoßes, spätestens jedoch binnen 24 Stunden ab Kenntnis (AK INC-02) – jede Verletzung des Schutzes personenbezogener Daten (Art. 4 Nr. 12 DSGVO) sowie jeden IT-Sicherheitsvorfall, der den Vertragsgegenstand betrifft. Verletzungen i. S. d. Art. 4 Nr. 12 DSGVO sind stets meldepflichtig.
- (2) Für die Meldung nutzt der Auftragnehmer das vordefinierte Standard-Meldetemplate, das die nach Art. 33 Abs. 3 DSGVO erforderlichen Angaben strukturiert enthält (AK INC-03). Der Auftragnehmer ergreift im Benehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten und zur Minderung nachteiliger Folgen und unterstützt den Auftraggeber bei dessen Melde- und Benachrichtigungspflichten (Art. 33, 34 DSGVO).
- (3) Der Auftragnehmer betreibt ein rund um die Uhr besetztes Security Incident Management (SOC) sowie automatisierte Mechanismen zur Angriffserkennung und -eindämmung; bei Kompromittierung eines Mandanten ist dessen sofortige Quarantäne ohne Lateral Movement auf andere Mandanten sicherzustellen (AK INC-01/04/05).

§ 9 Weisungsbefugnis des Auftraggebers (Art. 28 Abs. 3)

- (1) Der Umgang mit den Daten erfolgt ausschließlich im Rahmen dieser Vereinbarung und nach Weisung des Auftraggebers. Der Auftraggeber ist berechtigt, jederzeit Weisungen zu erteilen. Weisungen erfolgen grundsätzlich in Textform; mündliche Weisungen bestätigt der Auftraggeber unverzüglich in Textform.
- (2) Der Auftragnehmer führt ein Weisungsverzeichnis über alle erteilten Weisungen und legt es dem Auftraggeber auf Anfrage vor.

- (3) Hält der Auftragnehmer eine Weisung für datenschutzrechtswidrig, weist er den Auftraggeber unverzüglich darauf hin (Art. 28 Abs. 3 UAbs. 2 DSGVO) und darf ihre Durchführung bis zur Bestätigung oder Änderung aussetzen.
- (4) Erteilt der Auftraggeber Einzelweisungen bzgl. des Umgangs mit personenbezogenen Daten, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, z. B. Änderungen an den technischen und organisatorischen Maßnahmen, werden sie als Antrag auf Leistungsänderung behandelt. Weisungen, die zur Einhaltung datenschutzrechtlicher Pflichten erforderlich sind, führt der Auftragnehmer ohne gesondertes Entgelt aus. Nur Weisungen, die eine substantielle Erweiterung des vereinbarten Leistungsumfangs verlangen, können als Antrag auf Leistungsänderung behandelt werden.

§ 10 Löschung von Daten und Rückgabe von Datenträgern (Art. 28 Abs. 3 g)

- (1) Nach Wahl des Auftraggebers gibt der Auftragnehmer die Daten zurück oder löscht sie; vorhandene Kopien werden gelöscht, soweit nicht Unionsrecht oder mitgliedstaatliches Recht eine Speicherung verlangt. Ein über gesetzliche Aufbewahrungs- und revisionssichere Nachweispflichten hinausgehender Rückbehalt ist ausgeschlossen. Ein Zurückbehaltungsrecht besteht nicht.
- (2) Die Löschung folgt dem im Datenschutzkonzept vorgesehenen zweistufigen, quitierten Verfahren (DSK Ziff. 9.2/13; AK EXT-01/02/04)
- (3) Das Protokoll der Löschung ist auf Anforderung vorzulegen. Sicherungskopien, die zur Vertraulichkeit sicher aufzubewahren sind, werden zu dem festgelegten Zeitpunkt vernichtet. Nachweisdokumentationen der ordnungsgemäßen Verarbeitung sind über das Vertragsende hinaus nach den geltenden Aufbewahrungsfristen aufzubewahren.

§ 11 Datenverarbeitungen mittels Künstlicher Intelligenz

- (1) Verbotene Praktiken (Art. 5 KI-VO): Ausgeschlossen sind insbesondere die Ableitung von Emotionen von Prüflingen, Prüfern oder Aufsichten im Prüfungs- und Bildungskontext (Art. 5 Abs. 1 lit. f KI-VO), die biometrische Kategorisierung zur Erschließung sensibler Merkmale (Art. 5 Abs. 1 lit. g KI-VO) sowie manipulative Techniken und Social Scoring. Diese Praktiken sind technisch und organisatorisch auf der gesamten Plattform unterbunden (AK KI-01).
- (2) Hochrisiko-KI: KI-Systeme zur Bewertung von Prüfungsleistungen oder zur Überwachung von Prüflingen fallen als Bildungs-/Berufsbildungsanwendung grundsätzlich unter Anhang III KI-VO (Hochrisiko) und sind grundsätzlich ausgeschlossen. Ein Einsatz ist nur ausnahmsweise und kumulativ zulässig, wenn
 - (a) das System nachweislich kein erhebliches Grundrechtsrisiko birgt (Art. 6 Abs. 3 KI-VO, nur unterstützende/vorbereitende Teiltätigkeit ohne Notenvorschlag),
 - (b) die Anforderungen des Kapitels 2 KI-VO erfüllt sind und
 - (c) f für den konkreten Einsatz ein Betriebskonzept vorliegt, das von den Datenschutzbeauftragten geprüft und von der Geschäftsführung der betroffenen IHK freigegeben wurde (DSK Ziff. 14.2).
- (3) Menschliches Korrektiv (Art. 22 DSGVO): Eine ausschließlich automatisierte Einzelfallentscheidung bei der Notenermittlung ist unzulässig. Jeder KI-generierte Bewertungsvorschlag ist dem zuständigen menschlichen Prüfungsausschuss zur Prüfung, Abänderung und manuellen Freigabe vorzulegen; die Letztentscheidung verbleibt beim Menschen (AK KI-02).

- (4) Transparenz und Erklärbarkeit: Der Einsatz eines KI-Systems wird den Prüflingen vor Prüfungsbeginn in leicht verständlicher, barrierefreier Weise offengelegt (Art. 50 KI-VO). Das System begründet seine Vorschläge anhand der hinterlegten Musterlösungen und Bewertungskriterien nachvollziehbar (Explainable AI) (AK KI-03).
- (5) Mandantensteuerung: KI-Funktionen sind je IHK-Mandant aktivierbar (Opt-in) bzw. vollständig deaktivierbar (Opt-out). Bei Deaktivierung ist technisch sicherzustellen, dass keine Stamm- oder Prüfungsdaten dieses Mandanten an KI-Schnittstellen übertragen werden (AK KI-04).
- (6) Trainingsverbot: Die Nutzung personenbezogener Daten von Prüflingen oder Prüfern zum Training, Finetuning oder zur Weiterentwicklung von KI-Modellen des Auftragnehmers oder Dritter ist strikt untersagt (AK KI-05).
- (7) Daten-Governance und Sicherheit: Der Auftragnehmer weist Herkunft, Struktur und Repräsentativität der Trainingsdaten sowie Maßnahmen zur Bias-Minimierung nach (AK KI-06); bei generativen Modellen sind Validierungsmechanismen (z. B. RAG) zur Vermeidung von Halluzinationen vorzuschalten. Die Robustheit gegen Data Poisoning und Prompt Injection ist nachzuweisen (AK KI-07).

§12 Schlussbestimmungen

- (1) Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam sein oder werden oder eine Lücke enthalten, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, anstelle der unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem wirtschaftlichen Zweck der unwirksamen Regelung am nächsten kommt bzw. diese Lücke ausfüllt.
- (2) Änderungen und Ergänzungen bedürfen der Schriftform. Dies gilt auch für die Änderung dieser Schriftformklausel.
- (3) Beide Parteien verpflichten sich, über alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse, insbesondere über die bekannt gewordenen Daten, unter Beachtung des Betriebs- und Geschäftsgeheimnisses Stillschweigen zu bewahren. Diese Verpflichtung gilt auch nach Ende des Vertragsverhältnisses fort.
- (4) Es gilt deutsches Recht.
- (5) Ausschließlicher Gerichtsstand ist der Sitz des Auftraggebers (der jeweiligen IHK); der Auftraggeber kann den Auftragnehmer auch an dessen Sitz in Anspruch nehmen.

Unterschriften

Verantwortlicher (IHK)

Name: _____

Position: _____

Unterschrift: _____

Datum: _____

Auftragsverarbeiter

Name: _____

Firma: _____

Unterschrift: _____

Datum: _____

Anlage 1

Darstellung der technischen und organisatorischen Maßnahmen bei der Auftragsverarbeitung/Sicherheit der Verarbeitung

Unternehmen	
Stand	

1. Organisatorische Maßnahmen

- ☐ Ist ein betrieblicher Datenschutzbeauftragter bestellt?
 - ☐ ja
Name:
Kontaktdaten:
 - ☐ nein, dann bitte den Ansprechpartner für den Datenschutz angeben (Name, Kontaktdaten)
- ☐ Die Mitarbeiter wurden nachweislich über Datenschutz und Datensicherheit geschult bzw. informiert
- ☐ Alle Mitarbeiter sind nachweislich auf die Vertraulichkeit (Datengeheimnis), ggf. auf das Fernmeldegeheimnis und die Wahrung von Berufsgeheimnissen, verpflichtet
- ☐ Es existieren verfahrensunabhängige Plausibilitäts- und Sicherheitsprüfungen (z. B. technisch unterstützt oder durch Externe)
- ☐ Ein Datensicherheitskonzept/ Informationssicherheitsmanagement ist vorhanden
- ☐ Ein Datenschutzkonzept ist vorhanden
- ☐ Eine Auditierung/Zertifizierung ist vorhanden (Prüfung der Einhaltung am tt.mm.jjjj und Bestätigung s. Anlage x)
- ☐ Verhaltensregeln nach Art. 40 DSGVO sind vorhanden (Unterwerfung am tt.mm.jjjj und Bestätigung s. Anlage x)
- ☐ Ein dokumentierter Prozess zum Patch- und Schwachstellenmanagement ist vorhanden (regelmäßige Identifikation und zeitnahe Behebung bekannter Schwachstellen).
- ☐ Ein dokumentierter Prozess für sichere Softwareentwicklung bzw. Änderungs-/Freigabemanagement (Change Management) ist vorhanden.

2. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- ☐ Sind schriftliche Zutrittsregelungen vorhanden?
 - ☐ ja, im Dokument (z. B. im Datenschutzhandbuch):
 - ☐ nein
- ☐ Schriftliche Zutrittsregelungen zum Betreten des Rechenzentrums/der Räume mit DV-Anlagen sind vorhanden
- ☐ Alarmanlage
- ☐ Automatisches Zutrittskontrollsystem, Ausweisleser
- ☐ Türsicherung (elektrischer Türöffner, Zahlenschloss usw.)
- ☐ Schlüsselregelung (Schlüsselverwaltung: Schlüsselausgabe etc.)
- ☐ Sicherheitsschlösser
- ☐ Chipkarten-/Transponder-Schließsystem
- ☐ biometrische Kontrollsysteme (Fingerabdrücke o. ä.)
- ☐ Manuelles Schließsystem
- ☐ Schranken/Vereinzelungsanlagen (Drehkreuze o. ä.)
- ☐ Magnetschleusen
- ☐ Werkschutz/Pförtner
- ☐ Empfang mit Anmeldung
- ☐ Sorgfältige Auswahl von Wachpersonal
- ☐ Sorgfältige Auswahl von Reinigungspersonal
- ☐ Lichtschranke/Bewegungsmelder
- ☐ Feuerfeste Türen
- ☐ Absicherung von Gebäudeschächten
- ☐ Fenstervergitterung
- ☐ Panzerglas
- ☐ Videoüberwachung der Zugänge

2.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- ☐ Passwortvergabe
 - ☐ Komplexität des Passworts
 - ☐ Definierte Wechselfristen
 - ☐ Anzahl der Fehleingaben beschränkt
- ☐ Chipkarte mit PIN/Passwort
- ☐ Authentifikation mit Benutzername/Passwort
- ☐ Biometrisches Merkmal mit PIN/Passwort
- ☐ Einsatz von VPN-Technologie
- ☐ Automatische Sperrung des Arbeitsplatzes
- ☐ Nutzung von 2-Faktor-Authentifizierung für privilegierte Rollen (z. B. Prüfer, IHK-Mitarbeitende, Administratoren, Aufgabenersteller)
- ☐ automatische Sitzungsbeendigung bei Inaktivität
- ☐ Schutz vor unbefugter Nutzung von Benutzerkonten

2.3 Zugriffskontrolle

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

- ☐ Schriftliches Berechtigungskonzepts vorhanden
- ☐ Zuordnung von Benutzerrechten/Erstellen von Benutzerprofilen
- ☐ Verwaltung der Rechte durch System-Administrator
- ☐ Anzahl der Administratoren auf das "Notwendigste" reduziert
- ☐ Gesicherte Nutzung von USB-Schnittstellen
- ☐ Verschlüsselung von Smartphone-Inhalten
- ☐ Verschlüsselung von mobilen Datenträgern
- ☐ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
 - ☐ Die Protokolle werden ausgewertet, zeitlicher Abstand:
- ☐ physische Löschung von Datenträgern vor Wiederverwendung
- ☐ Einsatz von Akten-/Datenträgervernichtern bzw. Dienstleistern unter Beachtung von DIN 66399
- ☐ Verschlüsselung von Datenträgern
- ☐ Sichere Aufbewahrung von Datenträgern
- ☐ ordnungsgemäße Vernichtung von Datenträgern
- ☐ Lösungskonzept für Daten
- ☐ Protokollierung der Vernichtung
- ☐ Berechtigungen werden über ihren gesamten Lebenszyklus verwaltet (zeitnaher Entzug bei Rollenwechsel oder Ausscheiden, regelmäßige Rezertifizierung, gesonderte Absicherung privilegierter Zugänge).

2.4 Trennungskontrolle / Mandantentrennung

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- ☐ physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- ☐ Versehen der Datensätze mit Zweckattributen/Datenfeldern
- ☐ Logische Mandantentrennung (softwareseitig)
- ☐ Trennung von Produktiv- und Testsystem
- ☐ Festlegung Technologie von Datenbankrechten
- ☐ Trennung von Daten verschiedener Auftraggeber

2.5 Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass der Personenbezug von Daten nicht vollständig, aber immerhin so weit aufgelöst wird, dass ein Rückschluss auf eine bestimmte Person nur unter „Hinzuziehung zusätzlicher Informationen“, insbes. eines Identifizierungsschlüssels, möglich ist.

- ☐ Ja
- ☐ Nein

2.6 Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Die Verarbeitung und Speicherung („data at rest“) von personenbezogener Daten erfolgt in einer Weise, dass die Daten durch kryptografische Maßnahmen so verändert werden, dass sie – insbes. während ihres Übertragungsvorgangs – ohne den Schlüssel nicht mehr lesbar sind, ein unberechtigter Zugriff Dritter mithin ausgeschlossen ist.

- ☐ Ja (TLS 1.2 oder höher)
- ☐ Nein

- ☐ Es besteht ein dokumentiertes Schlüsselmanagement über den gesamten Lebenszyklus (Erzeugung, sichere Speicherung, Wechsel / Rotation, Vernichtung des Schlüsselmaterials).

3. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

3.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- ☐ Einrichtungen von Standleitungen bzw. VPN-Tunneln
- ☐ Firewall
- ☐ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form bzw. Verschlüsselung
- ☐ E-Mail-Verschlüsselung
- ☐ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
- ☐ Protokollierung von Übermittlungen
- ☐ Erstellen einer Übersicht von Datenträgern, Aus- und Eingang
- ☐ Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und Fahrzeugen
- ☐ Sicherung von Datenträgertransporten (verschießbarer Transportbehälter) auch für Papier

3.2 Eingabekontrolle/Verarbeitungskontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- ☐ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- ☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- ☐ Protokollauswertungsroutinen/-systeme vorhanden
- ☐ Aufbewahrungs-/Löschungsfrist für Protokolle vorhanden
- ☐ Protokollierung und Auswertung sicherheitsrelevanter Ereignisse (über die reine Zugriffsprotokollierung hinaus); Schutz der Protokolle vor nachträglicher Veränderung.

3.3 Dokumentationskontrolle

Maßnahmen, die gewährleisten, dass die Verfahrensweisen bei der Verarbeitung personenbezogener Daten in einer Weise dokumentiert werden, dass sie in zumutbarer Weise nachvollzogen werden können.

- ☐ Führung eines Verzeichnisses von Verarbeitungstätigkeiten
- ☐ Dokumentation der eingesetzten IT- Systeme und deren Systemkonfiguration
- ☐ Sichere Grundkonfiguration und Härtung der eingesetzten Systeme nach einem anerkannten Standard; Deaktivierung nicht benötigter Dienste.

3.4 Auftragskontrolle

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

- ☐ Vorhandene Vereinbarungen zur Auftragsdatenverarbeitung
- ☐ Kontrolle der Vertragsausführung
- ☐ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- ☐ Regelung zu Wartungen (speziell Fernwartung)

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

4.1 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- ☐ Unterbrechungsfreie Stromversorgung (USV)
- ☐ Überspannungsschutz
- ☐ Schutz gegen Umwelteinflüsse (Sturm, Wasser)
- ☐ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- ☐ Feuer- und Rauchmeldeanlagen
- ☐ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- ☐ Testen von Datenwiederherstellung
- ☐ Klimaanlage in Serverräumen
- ☐ Schutzsteckdosenleisten in Serverräumen
- ☐ Feuerlöschgeräte in Serverräumen
- ☐ Backups (Beschreibung von Rhythmus, Medium, Aufbewahrungszeit und -ort)
- ☐ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- ☐ Virenschutzsystem
- ☐ Spiegelung von Festplatten (z. B. RAID-Verfahren)
- ☐ Konzept für Katastrophenfall vorhanden

4.2 Belastbarkeit (Widerstandsfähigkeit/ Resilienz von Systemen/ Diensten)

Maßnahmen die gewährleisten, dass technische Systeme, bei Störungen bzw. Teil-Ausfällen nicht vollständig versagen, sondern wesentliche Systemdienstleistungen aufrechterhalten werden.

- ☐ Redundante Systemauslegung
- ☐ Ausfallsicherheits-/Hochverfügbarkeitskonzept
- ☐ Einsatz fehlertoleranter Software
- ☐ Schutz vor Überlast und Denial of Service-Angriffen
- ☐ Dokumentierte, regelmäßig überprüfte Wiederanlaufprozesse (Notfall- / Kontinuitätsmanagement) mit definierten Wiederanlaufzielen.

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

- ☐ Datenschutz-Management
- ☐ Incident-Response-Management
- ☐ Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Unterschriften

Verantwortlicher (IHK)

Name: _____

Position: _____

Unterschrift: _____

Datum: _____

Auftragsverarbeiter

Name: _____

Firma: _____

Unterschrift: _____

Datum: _____

Anlage 2

Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung folgender Subunternehmer durchgeführt:

Beschreibung der Teilleistungen (nicht abschließend)	Name und Anschrift des Subunternehmers
Hosting	
Webseiten-Design	
Cloud-Lösung	
Entsorgung von Akten/Datenträgern	

Anlage 3

Genaue Beschreibung des Verarbeitungsprozesses

1. Datenkategorien

2. Betroffener Personenkreis

3. Wie genau werden die personenbezogenen Daten verarbeitet? Ablauf der Verarbeitungsschritte?

Dummie 03_Verzeichnis-Unterauftragsverarbeiter-Muster