

# Datenschutzkonzept: Bundesweite digitale IHK-Prüfungsplattform

## 1. Einleitung und Zielsetzung

### 1.1 Ziel des Datenschutzkonzepts

Das vorliegende Datenschutzkonzept dient der systematischen Identifikation, Bewertung und Umsetzung der datenschutzrechtlichen und datensicherheitsrelevanten Anforderungen im Rahmen der Entwicklung, Bereitstellung und des Betriebs einer bundesweit eingesetzten digitalen Prüfungsplattform für die Organisation der Industrie- und Handelskammern (IHKs). Ziel ist es, eine vollumfänglich datenschutzkonforme, revisionssichere und rechtlich belastbare Verarbeitung personenbezogener Daten aller beteiligten Akteursgruppen – insbesondere von Prüflingen, Prüferinnen und Prüfern, Prüfungsaufsichten sowie Mitarbeitenden der IHKs – zu gewährleisten.

Darüber hinaus schafft dieses Konzept die verbindliche rechtliche und technische Grundlage für die Ausgestaltung der Leistungsbeschreibung, der Systemarchitektur sowie der vertraglichen Regelungen mit dem zukünftigen Plattformbetreiber. Es stellt sicher, dass Datenschutzanforderungen von Beginn an in den Beschaffungs- und Entwicklungsprozess integriert werden („*Privacy by Design*“ und „*Privacy by Default*“) und dient als verbindliche Leitlinie für den späteren produktiven Betrieb und die kontinuierliche funktionale Weiterentwicklung der Plattform.

### 1.2 Geltungsbereich und Abgrenzung

Dieses Konzept gilt für sämtliche Verarbeitungsprozesse personenbezogener Daten im Zusammenhang mit der Bereitstellung, dem Betrieb und der Migration der digitalen IHK-Prüfungsplattform. Es umfasst die Phasen der Prüfungsvorbereitung und -organisation, die technische Durchführung der Prüfungen sowie die nachgelagerte Korrektur, Bewertung und Ergebnisübermittlung.

Nicht Gegenstand dieses Konzepts sind Datenverarbeitungen, die außerhalb der Plattform in den lokalen Verwaltungssystemen (Vorsystemen) der einzelnen IHKs erfolgen, es sei denn, diese greifen unmittelbar über Schnittstellen (APIs) auf die Plattform zu. Ebenso sind die lokale Bereitstellung von Endgeräten (Hardware) vor Ort sowie die physische Netzwerkinfrastruktur in den Prüfungsräumen der IHKs nur insoweit erfasst, wie sie unmittelbare Schnittstellen- oder Sicherheitsauswirkungen auf die Nutzung der Plattform haben.

## 2. Beschreibung der Datenverarbeitung

### 2.1 Beteiligte Akteure und Rollen

Die rechtliche und funktionale Strukturierung der Akteure folgt einem klaren **Drei-Wege-Modell**, das eine unzulässige Haftungsdurchleitung an die DIHK ausschließt:

| Rolle / Akteur                           | Datenschutzrechtliche Rolle (DSGVO)                                      | Kurzbeschreibung im Plattformkontext                                                                                                                                                                                                                 |
|------------------------------------------|--------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Regionale IHKs (bis zu 79)</b>        | <b>Verantwortlicher</b> (Art. 4 Nr. 7 DSGVO)                             | Die einzelnen Kammern bestimmen als öffentlich-rechtliche Körperschaften Zwecke und Mittel der Datenverarbeitung für die von ihnen durchgeführten Prüfungen. Sie halten die alleinige Datenhoheit.                                                   |
| <b>DIHK</b>                              | <b>Koordinierender Dienstleister</b> (Keine operative Datenverarbeitung) | Die DIHK fungiert als zentrale Koordinierungsstelle (Shared Service). Sie verhandelt den Rahmenvertrag und stellt die Muster-DSFA bereit, verarbeitet jedoch standardmäßig <i>keine</i> personenbezogenen Prüfungsdaten ( <i>Zero-Data-Access</i> ). |
| <b>Plattformanbieter (Auftragnehmer)</b> | <b>Auftragsverarbeiter</b> (Art. 28 DSGVO)                               | Der Betreiber stellt die technische Plattform bereit und verarbeitet die Daten ausschließlich im Auftrag und nach Weisung der jeweils beitretenden regionalen IHK auf Basis eines direkt geschlossenen AVVs.                                         |
| <b>Subdienstleister (z. B.</b>           | <b>Unterauftragsverarbeitete</b>                                         | Vom Plattformbetreiber                                                                                                                                                                                                                               |

|                                                |                                                          |                                                                                                                                                                   |
|------------------------------------------------|----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Hoster)</b>                                 | <b>r (UAV)</b>                                           | vertraglich eingebundene Infrastruktur- oder Cloud-Dienstleister, die strengen Prüf- und Zustimmungsvorbehalten unterliegen.                                      |
| <b>Prüflinge</b>                               | <b>Betroffene Personen</b><br>(Art. 4 Nr. 1 DSGVO)       | Natürliche Personen, die an Prüfungen (z. B. nach dem BBiG) teilnehmen und deren Daten (Stamm-, Leistungs- und Protokolldaten) verarbeitet werden.                |
| <b>Prüferinnen / Prüfer</b>                    | <b>Funktionale Rolle / Betroffene</b>                    | Im Auftrag des Verantwortlichen handelnde Personen, die Bewertungen vornehmen. Ihre Nutzungs- und Protokolldaten unterliegen strikten Verwendungsbeschränkungen . |
| <b>Prüfungsaufsichten</b>                      | <b>Hilfspersonal / Betroffene</b>                        | Personen, die den ordnungsgemäßen Ablauf vor Ort überwachen und im System administrative und dokumentierende Handlungen vornehmen.                                |
| <b>IHK-Mitarbeitende</b>                       | <b>Interne Nutzer / Betroffene</b>                       | Mitarbeitende der IHK-Geschäftsstellen, die Prüfungen administrieren, Stammdaten importieren und Ergebnisse exportieren.                                          |
| <b>Aufgabenerstellungseinrichtungen (AEEs)</b> | Drittbeteiligte<br>(Verantwortliche für Prüfungsinhalte) | Stellen (z. B. AkA, ZPA, PAL), die Prüfungsaufgaben und Musterlösungen zuliefern. Ein Bezug zu personenbezogenen Daten besteht allenfalls                         |

|  |  |                                   |
|--|--|-----------------------------------|
|  |  | flüchtig über<br>Importmetadaten. |
|--|--|-----------------------------------|

## 2.2 Betroffenenkategorien und Schutzbedarf

Entsprechend der Sensibilität der Daten und den Risiken für die Rechte und Freiheiten der Personen werden folgende Kategorien definiert:

- **Prüflinge (Allgemein):** Stammdaten, Anmeldedaten, Prüfungsleistungen, Zeitstempel, Klickprotokolle. **Schutzbedarf: Hoch.** Ein Missbrauch oder Datenverlust beeinträchtigt den beruflichen Werdegang und die Existenzgrundlage unmittelbar.
- **Prüflinge mit besonderem Schutzbedarf (z. B. Minderjährige, Menschen mit Behinderung):** Untergruppe mit erhöhtem Schutzbedarf. Umfasst auch Daten zum Nachteilsausgleich (medizinische Einschränkungen). **Schutzbedarf: Hoch.**
- **Prüferinnen und Prüfer:** Stammdaten, Zuordnung zu Fachbereichen, vergebene Punkte, Protokolle der Bewertungsschritte. **Schutzbedarf: Normal** (Ausschluss der Verhaltens- und Leistungskontrolle).
- **Prüfungsaufsichten / IHK-Mitarbeitende / Aufgabenersteller:** Stammdaten, Authentifizierungsdaten, administrative Protokolle. **Schutzbedarf: Normal.**

## 2.3 Datenarten und Datenquellen

### Datenarten:

- **Stammdaten:** Vorname, Nachname, Geburtsdatum, Prüflingsnummer (Identifikationsnummer), Kammerzugehörigkeit.
- **Kontaktdaten:** E-Mail-Adresse, Mobilfunknummer (ausschließlich für die datenschutzrechtlich erforderliche 2-Faktor-Authentifizierung privilegierter Nutzer).
- **Zugangs- und Authentifizierungsdaten:** Benutzernamen, kryptografisch gesicherte Passwort-Hashes, Sitzungs-Tokens.
- **Organisations- und Prüfungsmetadaten:** Prüfungstermin, Prüfungsort, Raumzuordnung, zugewiesene Aufsichten und Prüfer, gewährte Schreibzeitverlängerungen.
- **Daten zum Nachteilsausgleich (besondere Kategorien personenbezogener Daten, Art. 9 Abs. 1 DSGVO):** Angaben über eine Behinderung oder gesundheitliche Einschränkung sowie hierzu vorgelegte Nachweise sind Gesundheitsdaten. Auf der Plattform werden ausschließlich die abstrakten Umsetzungsparameter des bewilligten Ausgleichs verarbeitet (z. B. „Schreibzeitverlängerung 25 %“, „Screenreader-Kompatibilität“, „Einzelraum“); Diagnosen, Attest-Inhalte und der Grad der Behinderung verbleiben in der Prüfungsakte der IHK. Einzelheiten regelt Ziff. 5.3.
- **Prüfungsleistungsdaten:** Abgegebene Freitextantworten, ausgewählte Multiple-Choice-Optionen, Zwischenstände, hochgeladene Prüfungsdateien, Zeitstempel je Aufgabe.

- **Bewertungs- und Ergebnisdaten:** Punktzahlen, fachliche Kommentare der Prüfer, Erst- und Zweitprüferentscheidungen, maschinell ermittelte Teilergebnisse, finale Notenvorschläge.
- **System- und Revisionsprotokolle (Audit Logs):** IP-Adressen (anonymisiert/verkürzt nach 7 Tagen), Login-Logs, exakte Klickpfad-Protokolle der Prüflinge (zur Abwehr von Täuschungsversuchen und zum Nachweis des rechtmäßigen Ablaufs bei Widerspruchsverfahren).

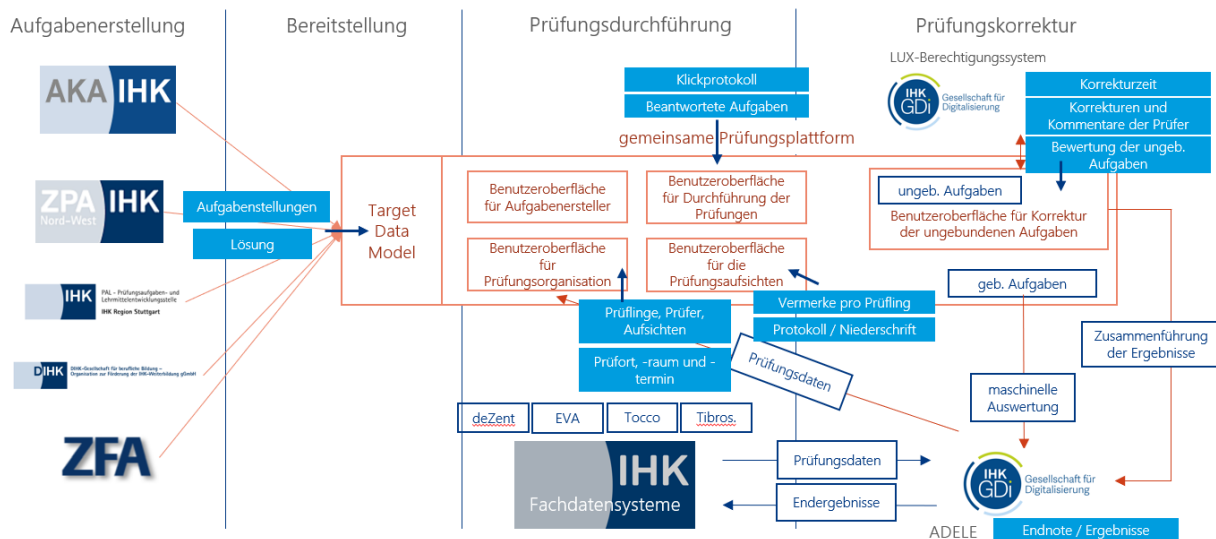
## Datenquellen & Schnittstellenpartner:

Die Daten fließen über definierte, gesicherte Schnittstellen in die Plattform ein und aus ihr ab:

- **Import von Stammdaten:** Aus den etablierten IHK-Verwaltungssystemen (**EVA, Tibros, DeZent, Tocco, Elvis/ADELE**).
- **Import von Prüfungsinhalten:** Aus den Systemen der Aufgabenerstellungseinrichtungen (**ASPE-Workbench (Aka), IHK-exam (DIHK Bildungs gGmbH), Christiani/PAL, ZPA Nord-West, ZFA**).
- **Zentrales Berechtigungssystem:** Authentifizierung über **LUX-BS (GDi)**.
- **Ergebnisexport:** Zurückführung der Rohnoten und Bewertungsprotokolle an das Vorsystem **ADELE (GDi)** zur endgültigen Notenverbuchung und Zeugniserstellung.

## 2.4 Verarbeitungsprozesse

### Datenerhebung und -verarbeitung



Der Lebenszyklus der Daten auf der Plattform gliedert sich in sechs chronologische Phasen:

[2.4.1 Organisation] -> Import der Stammdaten & Erstellung der Prüfungsumgebung (IHK-Mandant)

|

[2.4.2 Bereitstellung] -> Verschlüsselter Import der Aufgaben & Musterlösungen (AEs)

|

[2.4.3 Durchführung] -> Verschlüsselte Erfassung der Antworten, Klickprotokolle & Offline-Caching (Prüfling)

|

[2.4.4 Korrektur] -> Pseudonymisierte Bewertung der Freitextaufgaben durch Prüfer (Human-in-the-Loop)

|

[2.4.5 Logging/Export] -> Revisionssichere Protokollierung und Export der Ergebnisse nach ADELE

|

[2.4.6 Löschung] -> Quittierter Transfer der Archivdaten an die IHK, anschließende Löschung auf der Plattform

- **2.4.1 Prüfungsorganisation und Vorbereitung:** IHK-Mitarbeitende importieren die Stammdaten. Die Plattform generiert temporäre Zugangsdaten und pseudonyme Prüfungs-IDs. Die Daten verbleiben strikt im Datenraum des jeweiligen IHK-Mandanten.
- **2.4.2 Bereitstellung von Prüfungsinhalten:** Aufgaben werden importiert und bis zum exakten Prüfungsbeginn kryptografisch unter Verschluss gehalten. Der Zugriff ist softwareseitig (Ebene 2) gesperrt.
- **2.4.3 Durchführung der Prüfung:** Prüflinge melden sich an. Die Plattform erfasst Antworten in Echtzeit. Bei Netzunterbrechungen greift ein verschlüsseltes *Offline-Caching* im Browser des Prüflings (Ebene 2). Aufsichten überwachen den Status live über ein Dashboard.
- **2.4.4 Korrektur und Bewertung:** Die Plattform stellt den Prüfern die Freitextantworten zur Korrektur bereit. Dieser Prozess erfolgt **standardmäßig pseudonymisiert** (der Prüfer sieht keine Klarnamen). Notenkorrekturen werden revisionssicher historisiert.
- **2.4.5 Speicherung, Protokollierung und Nachvollziehbarkeit:** Systemseitig werden alle bewertungsrelevanten Aktionen protokolliert. Die Daten verbleiben als temporäre Arbeitskopie auf der Plattform.
- **2.4.6 Datenexport, Archivierung und Löschung:** Nach Abschluss der Prüfungskorrektur werden alle Daten (Prüfungsleistungen, Protokolle, Ergebnisse) strukturiert an die zuständige IHK exportiert. Erst nach kryptografischer Empfangsbestätigung (*Quittierung*) durch die IHK wird die Löschkette auf der Plattform in Gang gesetzt.

### 3. Schutzbedarfsanalyse

### 3.1 Klassifizierung der Daten

Die Klassifizierung bestimmt die Schärfe der technischen und organisatorischen Schutzmaßnahmen (TOM):

- **Normaler Schutzbedarf:** Einfache Organisationsdaten, Kontaktdaten zur Terminabsprache, administrative Standard-Logs.
- **Hoher Schutzbedarf:** \* Authentifizierungsdaten (MFA-Tokens, Passwörter).
  - Prüfungsaufgaben und Musterlösungen vor der Prüfung (Gefahr der Prüfungsunbrauchbarkeit bei Leak).
  - Tatsächliche Prüfungsleistungen und Klickprotokolle der Prüflinge (Beweismittel im Widerspruchsverfahren).
  - Bewertungsentscheidungen und finale Ergebnisdaten.
  - Personenbezogene Daten minderjähriger Prüflinge.

### 3.2 Risikomatrix nach Gewährleistungszielen

Die Risikoanalyse bewertet die potenziellen Auswirkungen von Verstößen gegen die sieben grundlegenden Gewährleistungsziele des Datenschutzes:

| Gewährleistungsziel    | Identifiziertes Risiko im Prüfungskontext                                        | Mögliche Auswirkung für den Betroffenen                                                              |
|------------------------|----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| <b>Vertraulichkeit</b> | Unbefugter Zugriff auf Aufgaben vorab oder Prüfungsleistungen Dritter.           | Notwendigkeit des bundesweiten Prüfungsabbruchs, Verletzung der Privatsphäre, Chancennachteil.       |
| <b>Integrität</b>      | Manipulation von Noten oder nachträgliche Veränderung von abgegebenen Antworten. | Ungerechtfertigtes Nichtbestehen oder unverdiente Zertifizierung; rechtliche Angreifbarkeit der IHK. |
| <b>Verfügbarkeit</b>   | Systemausfall während einer synchronen, bundesweiten Prüfung (Lastspitze).       | Massiver Prüfungsabbruch, psychische Belastung der Prüflinge, Schadensersatzforderungen gegen IHKs.  |

|                           |                                                                                                 |                                                                                          |
|---------------------------|-------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| <b>Datenminimierung</b>   | Übermäßige Erfassung von Nutzungsdaten (z. B. permanente biometrische Videoanalyse).            | Unzulässige Überwachung, Verstoß gegen den Grundsatz der Verhältnismäßigkeit.            |
| <b>Nichtverkettung</b>    | Zusammenführung von Prüfungsdaten mit allgemeinen IHK-Mitgliederdaten oder Registern.           | Zweckentfremdung der Daten, Erstellung unzulässiger Persönlichkeitsprofile.              |
| <b>Transparenz</b>        | Intransparente (teil-)automatisierte Notenvorschläge oder unklare Datenflüsse über APIs.        | Unmöglichkeit der effektiven Rechtsverteidigung gegen Prüfungsentscheidungen.            |
| <b>Intervenierbarkeit</b> | Unmöglichkeit, Systemfehler manuell zu korrigieren oder Daten bei Fehlübertragungen zu sichern. | Endgültiger Datenverlust, Verletzung des Rechts auf den gesetzlichen Nachteilsausgleich. |

### 3.3 Besondere Risikofaktoren

- **Bundesweite Lastspitzen:** Bis zu zehntausende Prüflinge greifen zeitgleich sekundengenau auf die Plattform zu. Dies erfordert ein hochperformantes, elastisches Hosting, das die Datensicherheit auch unter Volllast garantiert.
- **Mandantenfähigkeit:** Da 79 eigenständige IHKs dieselbe Plattform nutzen, ist eine fehlerhafte logische Abgrenzung der Datenbestände ein existentielles Risiko (Gefahr des unbefugten kammerübergreifenden Datenzugriffs).

## 4. Verantwortlichkeiten und Rollen

Das rechtliche Fundament der Plattformnutzung schließt eine unklare Haftungssituation aus:

### 4.1 Die regionalen IHKs als alleinige Verantwortliche

Jede der bis zu 79 regionalen IHKs entscheidet eigenständig über die Durchführung ihrer Prüfungen. Sie ist **alleiniger Verantwortlicher** gemäß Art. 4 Nr. 7 DSGVO für die Daten ihrer Prüflinge, Prüfer und Aufsichten. Sie erfüllt die gesetzlichen Betroffenenrechte und ist Ansprechpartner für die jeweils zuständige Landes-Datenschutzbehörde.

## 4.2 Die DIHK als reine Koordinierungsstelle

Die DIHK schließt als koordinierender Dienstleister den zentralen Rahmenvertrag mit dem Plattformanbieter ab, um wirtschaftliche und technische Synergien zu heben. Sie hat **keine eigene datenschutzrechtliche Verfügungsmacht** über die Prüfungsdaten und standardmäßig keinen Zugriff auf die Fachapplikation (Ebene 2) oder das Hosting (Ebene 3). Eine gemeinsame Verantwortlichkeit (Art. 26 DSGVO) der DIHK mit den IHKs für den allgemeinen Prüfungsbetrieb besteht *nicht*.

## 4.3 Die vertragliche Direkt-Koppelung

- Jede IHK tritt dem Rahmenvertrag per Beitrittserklärung bei.
- Gleichzeitig unterzeichnet jede IHK den **standardisierten Muster-AVV** direkt mit dem Plattformanbieter.
- Der Plattformanbieter haftet somit als Auftragsverarbeiter direkt gegenüber der jeweiligen IHK. Die DIHK ist aus dieser Haftungskette vollständig entkoppelt.

# 5. Rechtmäßigkeit der Verarbeitung

## 5.1 Rechtsgrundlagen

- **Erfüllung einer rechtlichen Verpflichtung / Hoheitliche Aufgabe (Art. 6 Abs. 1 lit. c und e DSGVO):** Der ganz überwiegende Teil der Datenverarbeitung dient der ordnungsgemäßen Vorbereitung, Durchführung und Bewertung von Prüfungen der beruflichen Bildung. Die gesetzliche Ermächtigung ergibt sich aus dem Berufsbildungsgesetz (BBiG) i.V.m. den einschlägigen Ausbildungs- und Prüfungsordnungen der jeweiligen Kammer sowie ergänzend aus § 1 Abs. 2 IHKG. . Diese Datenverarbeitungen können ergänzend auf Art. 6 Abs. 1 lit.e DSGVO i.V.m. § 1 Abs. 2 IHKG gestützt werden. Die nach Art. 6 Abs. 3 lit. b DSGVO erforderliche mitgliedstaatliche Rechtsgrundlage ergibt sich aus § 47 Abs. 1 und 2 BBiG in Verbindung mit der jeweiligen – von der obersten Landesbehörde genehmigten – Prüfungsordnung der IHK, für das Verzeichnis der Berufsausbildungsverhältnisse aus § 34 BBiG, sowie aus der allgemeinen Verarbeitungsbefugnis des jeweils anwendbaren Landesdatenschutzgesetzes. § 1 Abs. 2 IHKG weist den IHKs die Aufgabe zu, Maßnahmen zur Förderung und Durchführung der kaufmännischen und gewerblichen Berufsbildung zu treffen; die Norm ist eine Aufgabenzuweisung und genügt für sich allein nicht den Bestimmtheitsanforderungen des Art. 6 Abs. 3 DSGVO. Sie wird daher nur ergänzend herangezogen.
- **Vertragliche Erfüllung (Art. 6 Abs. 1 lit. b DSGVO):** Soweit Prüfungen außerhalb des hoheitlichen BBiG-Rahmens durchgeführt werden (z. B. zertifizierte Weiterbildungskurse auf privatrechtlicher Basis), dient die Verarbeitung der Erfüllung des Prüfungsvertrags mit dem Teilnehmer.
- **Berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO):** Diese Rechtsgrundlage ist für die

IHKs als öffentliche Stellen bei der Wahrnehmung ihrer hoheitlichen Aufgaben gemäß **Art. 6 Abs. 1 Unterabsatz 2 DSGVO ausdrücklich ausgeschlossen** und kommt allenfalls für Datenverarbeitungen in Betracht, die die jeweilige IHK im Rahmen zusätzlicher Leistungsangebote außerhalb ihrer öffentlich-rechtlichen Pflichten vornimmt.

## 5.2 Einwilligung und Widerrufsmanagement

Da Prüfungen rechtlich und organisatorisch verpflichtend sind und kein echtes Freiwilligkeitsverhältnis besteht, ist die **Einwilligung (Art. 6 Abs. 1 lit. a DSGVO) als primäre Rechtsgrundlage ungeeignet**.

Sollten für optionale Zusatzdienste auf der Plattform ausnahmsweise Einwilligungen eingeholt werden, müssen diese die strengen Anforderungen des Art. 7 DSGVO (gegebenenfalls i.V.m. Art. 8 DSGVO – dieser gilt allerdings nur für Dienste der Informationsgesellschaft, die auf einer Einwilligung beruhen, und damit nicht für den hoheitlichen Prüfungsbetrieb) und des § 25 Abs. 1 TDDDG erfüllen. Für technisch zwingend erforderliche Zugriffe auf die Endeinrichtung des Prüflings – insbesondere Sitzungs-Tokens und das verschlüsselte Offline-Caching nach Ziff. 11.2 – greift die Ausnahme des § 25 Abs. 2 Nr. 2 TDDDG; die Erforderlichkeit ist je Speichervorgang zu dokumentieren und im Rahmen der Abnahme zu verifizieren. Reichweitenmessung, Komfort- oder Analysefunktionen unterliegen dagegen dem Einwilligungserfordernis des § 25 Abs. 1 TDDDG und sind auf der Prüfungsoberfläche unzulässig. Die Plattform muss hierfür ein granulares, nachweisbares Einwilligungs- und Widerrufsmanagement auf Anwendungsebene (Ebene 2) bereitstellen.

## 5.3 – Verarbeitung von Daten zum Nachteilsausgleich

Zur Wahrung der Chancengleichheit im Prüfungsverfahren verarbeiten die IHKs Daten zur Feststellung, Bemessung, Gewährung, technischen Umsetzung und Dokumentation von Nachteilsausgleichen, insbesondere zur Verlängerung der Prüfungszeit, zur Zulassung von Hilfsmitteln, zu Assistenzleistungen einschließlich Gebärdensprachdolmetschung, zu gesonderten Prüfungsräumen und zur barrierefreien Aufgabendarstellung. Verantwortlich ist ausschließlich die jeweils prüfende IHK; der Plattformanbieter verarbeitet diese Daten allein als Auftragsverarbeiter nach Art. 28 DSGVO.

Die Verarbeitung der Antrags-, Organisations- und Umsetzungsdaten – Antragstellung, Bewilligungsentscheidung, gewährte Ausgleichsart und deren Umfang sowie die Steuerungsparameter der Plattform – erfolgt nach Art. 6 Abs. 1 Unterabs. 1 lit. e i. V. m. Abs. 2 und Abs. 3 lit. b DSGVO. Die mitgliedstaatliche Rechtsgrundlage ergibt sich aus § 65 Abs. 1 BBiG, der ausdrücklich die „Dauer von Prüfungszeiten, die Zulassung von Hilfsmitteln und die Inanspruchnahme von Hilfeleistungen Dritter wie Gebärdensprachdolmetscher für hörbehinderte Menschen“ erfasst, in Verbindung mit § 9 und § 47 Abs. 1 und 2 BBiG und den

hierauf gestützten Prüfungsordnungen der jeweiligen IHK sowie der allgemeinen Verarbeitungsbefugnis des anwendbaren Landesdatenschutzgesetzes (z. B. Art. 4 Abs. 1 BayDSG; weitere Länder siehe Anlage „Öffnungsnormen-Matrix“). Beruht ein Nachteilsausgleich nicht auf einer Behinderung, sondern auf einer vorübergehenden Beeinträchtigung – etwa einer akuten Erkrankung oder Verletzung – oder auf Mutterschutz, tragen die Prüfungsordnung und der Grundsatz der Chancengleichheit (Art. 3 Abs. 1, Art. 12 Abs. 1 GG) die Verarbeitung; § 65 Abs. 1 BBiG ist insoweit nicht einschlägig.

Bei der Rechtsgrundlage für besondere Kategorien personenbezogener Daten ist wie folgt zu unterscheiden. Angaben über eine Behinderung, gesundheitliche Einschränkungen sowie die hierzu vorgelegten Nachweise – ärztliche Bescheinigungen, Schwerbehindertenausweis, sonderpädagogische Gutachten – sind Gesundheitsdaten im Sinne des Art. 9 Abs. 1 DSGVO. Ihre Verarbeitung ist zulässig

- **vorrangig nach Art. 9 Abs. 2 lit. b DSGVO**, weil sie erforderlich ist, damit die betroffene Person die ihr aus dem Recht des Sozialschutzes erwachsenden Rechte – den Anspruch auf Berücksichtigung ihrer besonderen Verhältnisse nach § 65 Abs. 1 BBiG und auf Zulassung zur Abschlussprüfung nach § 65 Abs. 2 BBiG – ausüben und die IHK ihre entsprechenden Pflichten erfüllen kann, in Verbindung mit der landesrechtlichen Erlaubnisnorm
- **hilfsweise nach Art. 9 Abs. 2 lit. g DSGVO**, soweit das anwendbare Landesrecht die Verarbeitung aus Gründen eines erheblichen öffentlichen Interesses erlaubt und angemessene sowie spezifische Maßnahmen zur Wahrung der Grundrechte vorsieht;
- **subsidiär nach Art. 9 Abs. 2 lit. a DSGVO** (ausdrückliche Einwilligung), soweit keine der vorstehenden Erlaubnisnormen greift. Die Freiwilligkeit ist gewahrt, weil der Nachteilsausgleich auf Antrag der betroffenen Person gewährt wird und die Verweigerung oder der Widerruf der Einwilligung ausschließlich den Nachteilsausgleich, nicht aber die Zulassung zur oder die Teilnahme an der Prüfung berührt. Die Einwilligung ist, soweit landesrechtlich vorgeschrieben (z. B. § 16 Abs. 2 DSG NRW), schriftlich einzuholen; über die Widerruflichkeit mit Wirkung für die Zukunft nach Art. 7 Abs. 3 DSGVO ist zu informieren. Ein Widerruf nach Beginn der Prüfung berührt die Rechtmäßigkeit der bereits erfolgten Verarbeitung nicht.

Art. 9 Abs. 2 lit. b und lit. g DSGVO sowie die landesrechtlichen Erlaubnisnormen verlangen angemessene und spezifische Schutzmaßnahmen (§ 15 DSG NRW; Maßnahmenkatalog entsprechend § 22 Abs. 2 BDSG). Umgesetzt werden mindestens:

- Datenminimierung durch Parametrisierung: An die Plattform werden ausschließlich die Umsetzungsparameter des bewilligten Nachteilsausgleichs übertragen. Diagnosen, Attest-Inhalte, Grad der Behinderung und medizinische Nachweise werden nicht auf der Plattform verarbeitet; sie verbleiben im Vorsystem bzw. in der Prüfungsakte der

IHK.

- Kein Klartextbezug für Prüfer und Aufsichten: Prüferinnen und Prüfer erhalten keine Information über Grund oder Anlass des Nachteilsausgleichs; Aufsichten erhalten nur die zur Durchführung zwingend erforderliche Angabe, etwa eine veränderte Bearbeitungszeit.
- Verschlüsselung und Pseudonymisierung nach Ziff. 11.2 und 11.3, mit gesondertem Schlüsselmaterial für Nachteilsausgleichsdaten.
- Zweckbindung (Art. 5 Abs. 1 lit. b DSGVO): Eine Verwendung für die Leistungsbewertung, für Statistik, für Vergleichsauswertungen oder als Trainingsdaten für KI-Systeme ist ausgeschlossen.
- Löschung: Die Umsetzungsparameter werden mit der Prüfungsakte exportiert und nach Ziff. 9.2 auf der Plattform gelöscht.

## 6. Transparenz und Informationspflichten

### 6.1 Datenschutzerklärungen und Verlinkung („One Click Away“)

Die Erfüllung der Informationspflichten nach Art. 13 und 14 DSGVO erfolgt mandantenspezifisch. Da die IHKs unterschiedlichen Landes-Datenschutzgesetzen unterliegen, muss die Plattform technisch in der Lage sein, für jeden IHK-Mandanten eine **individuell anpassbare Datenschutzerklärung** darzustellen. Diese muss für den Nutzer in jedem Bereich der Benutzeroberfläche (z. B. im Footer der Anmelde- und Prüfungsscreen) mit nur einem Klick („one click away“) barrierefrei erreichbar sein.

### 6.2 Die Muster-Datenschutz-Folgenabschätzung (Muster-DSFA)

Aufgrund der großskaligen und hochriskanten Verarbeitung (Bewertung der beruflichen Eignung, Minderjährige, detailliertes Verhaltenslogging zur Täuschungsabwehr) ist eine **DSFA nach Art. 35 DSGVO zwingend erforderlich**.

Um den administrativen Aufwand für die 79 IHKs zu minimieren, wird folgendes Verfahren etabliert:

1. Der Plattformanbieter wird vertraglich verpflichtet, bei der Erstellung einer **Muster-DSFA** unter Mitwirkung der DIHK aktiv mitzuwirken.
2. Diese Muster-DSFA enthält die vollständige technische Risikoanalyse (Ebene 2 und 3).
3. Die regionalen IHKs übernehmen diese Muster-DSFA, passen sie an ihre lokalen organisatorischen Gegebenheiten (Ebene 1 - Fachverfahren) an und dokumentieren die Freigabe unter Einbindung ihrer lokalen Datenschutzbeauftragten.

## 7. Betroffenenrechtenmanagement

Die Wahrung der Rechte betroffener Personen (Auskunft, Berichtigung, Löschung, Einschränkung) obliegt der jeweils verantwortlichen IHK.

- **Recht auf Datenkopie (Art. 15 Abs. 3 DSGVO):** Die Fachapplikation (Ebene 2) muss eine automatisierte Exportfunktion bereitstellen. IHK-Mitarbeitende müssen auf Knopfdruck eine strukturierte, maschinenlesbare und gängige Datenkopie aller über einen Prüfling gespeicherten Daten (einschließlich seiner Klickprotokolle, Freitextantworten und Korrekturkommentare) generieren können. Das Exporttool muss eine Schwärzungsfunktion enthalten, um Rechte Dritter (z. B. Identität der Prüfer nach Art. 15 Abs. 4 DSGVO) zu schützen.
- **Einzellöschung und Sperrung:** Sollte ein Prüfling während eines laufenden Verfahrens (z. B. Widerspruch) die Sperrung seiner Daten verlangen, muss die Applikation das Setzen eines *Sperr-Flags* erlauben, das diese Daten von automatisierten Löschroutinen des Löschkonzepts ausnimmt.

## 8. Zweckbindung und Datenzugriff

### 8.1 Striktes Verbot der Mitarbeiterüberwachung

Sämtliche im Rahmen der Prüfungsdurchführung und -korrektur generierten Nutzungs-, Klick- und Bearbeitungsdaten von Prüferinnen, Prüfern, Aufsichten und IHK-Mitarbeitenden dienen **ausschließlich der Gewährleistung der Revisionssicherheit** von Prüfungsanfechtungen sowie der technischen Integrität des Plattformbetriebs (SOC). Eine Auswertung dieser Daten zur personal-, arbeits- oder dienstrechtlichen Leistungs- und Verhaltenskontrolle der Beschäftigten oder ehrenamtlich Tätigen ist softwareseitig und organisatorisch **strikt ausgeschlossen und unzulässig**.

### 8.2 Mandantentrennung auf drei Ebenen

Zur Gewährleistung der Trennungskontrolle (Verhinderung unbefugter kammerübergreifender Zugriffe) wird eine strikte Mandantentrennung implementiert:

- **Ebene 1 (Fachverfahren):** Organisatorische Schulung der Mitarbeiter; strikte Zuweisung von Benutzeraccounts ausschließlich zu ihrer jeweiligen IHK.
- **Ebene 2 (Fachapplikation):** *Tenant-Aware Software-Design*. Alle Datenbankabfragen und API-Aufrufe sind im Quellcode hartcodiert an die Mandanten-ID des angemeldeten Benutzers gekoppelt. Mandantenübergreifende Abfragen sind softwareseitig unmöglich.
- **Ebene 3 (Technische Infrastruktur):** Trennung der Datenbestände auf Datenbankebene (z. B. durch dedizierte logische Datenbankschemata mit **eigenen kryptografischen Schlüsseln pro IHK-Mandant**).

## 9. Datenminimierung und Speicherbegrenzung

### 9.1 Das temporäre Daten-Löschmodell

Die digitale Prüfungsplattform ist als **temporäres Verarbeitungssystem** konzipiert. Die dauerhafte Speicherung und rechtliche Archivierung der Prüfungsakten erfolgt ausschließlich in den lokalen IT-Systemen der jeweiligen regionalen IHK.

[Prüfungsphase abgeschlossen] -> [Export der PDF-Prüfungsakte an IHK] -> [Kryptografische Quittung der IHK] -> [90 Tage Karenzzeit (Sperrung)] -> [Physischer Shredder-Vorgang]

## 9.2 Der quitierte Löschprozess

1. Nach Ende eines Prüfungsfensters bzw. der Prüfungskorrektur (z. B. Frühjahrsprüfung) exportiert die IHK-Prüfungsorganisation alle prüfungsrelevanten Daten (Ergebnisse, Klickprotokolle, PDF-Prüfungsakten).
2. Der Plattformanbieter darf die Daten auf der Plattform erst dann löschen, wenn sichergestellt ist, dass die empfangende IHK die Daten vollständig erhalten hat. Es sollte im Laufe des Projekts geprüft werden, durch welche technischen Maßnahmen eine entsprechende Bestätigung erfolgen kann. Idealerweise sollte das Zielsystem der empfangenden IHK (z. B. ADELE) den fehlerfreien Empfang und die Validität der Daten kryptografisch quittieren
3. Nach erfolgreicher Quittierung werden die Daten auf der Plattform für den regulären Zugriff gesperrt (**Stufe 1: Sperrung**).
4. Nach Ablauf einer vertraglich vereinbarten Karenzzeit von **90 Tagen** (zur Absicherung gegen Übertragungsfehler oder sofortige Widersprüche) erfolgt die unwiderrufliche, physische Löschung der Daten auf den Servern und Backups der Plattform (**Stufe 2: Löschung**).

## 10. Drittstaatentransfers, Cloudbetrieb und Digitale Souveränität

Jede Übermittlung personenbezogener Daten an ein Drittland ist nur zulässig, wenn die Bedingungen des Kapitels V der DSGVO eingehalten werden (Art. 44 DSGVO). Als Übermittlung gilt auch der bloße Zugriff aus einem Drittland, etwa im Rahmen von Fernwartung oder Support. Zulässige Instrumente sind ein Angemessenheitsbeschluss der Kommission (Art. 45 DSGVO) oder geeignete Garantien nach Art. 46 DSGVO, insbesondere die Standarddatenschutzklauseln, jeweils ergänzt durch die nach der Rechtsprechung erforderlichen zusätzlichen Maßnahmen.

Um die Lastspitzen bundesweiter Prüfungstermine elastisch abzufangen, ist ein Cloud-Betrieb erforderlich. Da die IHKs hoheitliche Aufgaben wahrnehmen, gelten für den Cloudbetrieb strengste Souveränitätsregeln:

### 10.1 Geografische Restriktion (EU-Souveränität)

Sämtliche personenbezogenen Daten müssen als ruhende Daten (*data at rest*) ausschließlich in

Rechenzentren innerhalb der Europäischen Union (EU) bzw. des Europäischen Wirtschaftsraums (EWR) verarbeitet werden.

Dies sollte nach Möglichkeit auch für Daten im Arbeitsspeicher (data in use) und für alle Support-, Wartungs- und Administrationszugriffe (Fernwartung) sichergestellt sein. Ein Follow-the-Sun-Support ist ausgeschlossen. Support-Mitarbeiter außerhalb der EU bzw. des EWR dürfen weder Zugriff auf Serverkomponenten noch auf personenbezogene Daten oder sonstige Daten im Klartext erhalten. Sämtliche administrativen Dienstleistungen sind ausschließlich physisch aus Mitgliedstaaten der EU oder des EWR zu erbringen.

## 10.2 Zulässige Cloud-Betriebsmodelle im Vergabeverfahren

Das Vergabeverfahren bewertet die angebotenen Hosting-Infrastrukturen nach ihrer digitalen Souveränität:

- **Sovereign Cloud / Private Cloud (Bevorzugtes Zielmodell - High Scoring):** Plattformen, die auf rein europäischen Cloud-Infrastrukturen betrieben werden und keinerlei außereuropäischer Jurisdiktion (z. B. US Cloud Act) unterliegen.
- **Public Cloud (Zulässiges Modell nur unter strengen technischen Auflagen):** US-geprägte Hyperscaler (z. B. AWS, Azure, Google Cloud) sind nur dann zulässig, wenn sie die Risiken unbefugter Drittstaatentransfers durch hinreichende zusätzliche Garantien im Sinne der Rechtsprechung des Europäischen Gerichtshofes (Urteil vom 16. Juli 2020, Rechtssache C-311/18 -*Data Protection Commissioner gegen Facebook Ireland Ltd und Maximillian Schrems*) und der Empfehlungen des Europäischen Datenschutzausschusses (EDSA) sowie der Datenschutzkonferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) unter Berücksichtigung des jeweiligen Schutzbedarfs der verarbeiteten personenbezogenen Daten auf ein zu vernachlässigendes Restrisiko minimieren.

## 10.3 Technische Mindestanforderungen für den Public-Cloud-Betrieb

1. **Hold Your Own Key (HYOK) / Bring Your Own Key (BYOK):** Starke Verschlüsselung aller sensiblen Daten im Ruhezustand (*data at rest*). Die Schlüsselverwaltung und die Hoheit über die Entschlüsselung müssen nachweislich außerhalb der Cloud-Infrastruktur im exklusiven Einflussbereich der IHK-Organisation (oder eines europäischen Treuhänders) liegen. Alternative Schutzmaßnahmen sind möglich, sofern sie ein vergleichbares Schutzniveau in Bezug auf Drittstaatentransfers gewährleisten.
2. **Transfer Impact Assessment (TIA):** Jeder Bieter, der eine Public-Cloud-Infrastruktur mit Drittlandsbezug anbietet, muss ein detailliertes, lückenloses TIA vorlegen, das nachweist, dass unbefugte behördliche Zugriffe (z. B. unter FISA Sec. 702) durch die implementierten TOMs technisch unmöglich gemacht werden.

## 11. Technische und organisatorische Maßnahmen (TOM)

Die Umsetzung der TOMs folgt einem strukturierten **Drei-Ebenen-Modell** (Ebene 1: Fachverfahren, Ebene 2: Fachapplikation, Ebene 3: Technische Infrastruktur), abgebildet auf die sieben gesetzlichen Gewährleistungsziele des Datenschutzes:

### 11.1 Ebene 1: Fachverfahren (Organisatorisch-prozessuale Maßnahmen)

- **Vertraulichkeit:** \* Schriftlich fixierte Prozesse zur lückenlosen Identitätskontrolle der Prüflinge vor Ort (Abgleich mit Lichtbildausweisen) unter Ausschluss unbefugter Dritter.
  - Schriftliche Verpflichtung aller ehrenamtlichen Prüferinnen, Prüfer und Aufsichten auf das Datengeheimnis und spezifische Verhaltensregeln im Umgang mit digitalen Endgeräten.
- **Integrität:** \* Handschriftliche oder lokal getrennt erfasste Prüfungsniederschrift durch die Aufsicht zur Revisionssicherung von Vorkommnissen (Täuschung, technische Störungen).
  - Büroseitige Verifikationsprozesse bei der manuellen Erfassung oder Änderung von Stammdaten in den IHK-Vorsystemen vor dem Import.
- **Verfügbarkeit:** \* Bereitstellung detaillierter, lokaler Notfallpläne (z. B. Bereithalten von papiergebundenen Notfall-Prüfungssätzen für den Fall eines kompletten Strom- oder Netzausfalls vor Ort).
- **Datenminimierung:** \* Prozessuale Vorgabe, Prüfungsanmeldedaten erst zu dem Zeitpunkt zu importieren, an dem dies für die Erstellung der Prüfungsumgebung zwingend erforderlich ist.
- **Nichtverkettung:** \* Striktes Verbot der Nutzung von Prüfungsplattformdaten für statistische Zwecke oder Vergleiche außerhalb des gesetzlichen Auftrags des BBiG.
- **Transparenz:** \* Aushändigung von detaillierten Informationsblättern (Datenschutzhinweise nach Art. 13/14 DSGVO) bereits mit der Einladung zur Prüfung.
- **Intervenierbarkeit:** \* Etablierung eines standardisierten Prozesses zur Einreichung und Bewilligung von Nachteilsausgleichen und deren rechtzeitige Einpflege in die Plattformsteuerung.

### 11.2 Ebene 2: Fachapplikation (Software- und Anwendungsbezogene Maßnahmen)

- **Vertraulichkeit:** \* *Rollenbasierte Zugriffskontrolle (RBAC):* Im Quellcode hart codierte Funktionstrennung. Prüfer haben keinen Zugriff auf Admin-Funktionen; Prüflinge sehen ausschließlich ihre eigene Prüfung.
  - *Multi-Faktor-Authentifizierung (MFA):* Zwingende 2FA für alle administrativen und bewertenden Rollen (IHK-Mitarbeiter, Prüfer, Aufsichten, IT-Admins).

- *Sitzungsmanagement*: Automatisches Timeout aktiver Sitzungen nach 10 Minuten Inaktivität bei Aufsichten und 15 Minuten bei Prüfern.
- **Integrität**: \* *Kryptografische Abgabesicherung*: Automatische Erzeugung eines SHA-256-Hashes über alle Antworten des Prüflings unmittelbar bei der Abgabe zur Erkennung nachträglicher Manipulationen.
  - *Input-Validierung*: Absicherung aller Eingabefelder gegen SQL-Injections und Cross-Site-Scripting (XSS).
- **Verfügbarkeit**: \* *Offline-Caching*: Lokale, verschlüsselte Zwischenspeicherung der Antworten im Browser des Prüflings (IndexedDB) bei temporärem Netzwerkausfall mit automatischer Hintergrund-Synchronisation bei Netzwiederkehr.
- **Datenminimierung**: \* *Pseudonymisierte Korrekturmasken*: Die Software zeigt den Prüfern bei der Freitextkorrektur standardmäßig keine Klarnamen oder demografische Daten der Prüflinge, sondern ausschließlich eine temporäre Prüfungs-ID.
  - *Technische Identitätstrennung*: Die Zuordnungstabelle zwischen Klarnamen und Prüfungs-ID ist kryptografisch gekapselt und ausschließlich für die Rolle „Prüfungsaufsicht vor Ort“ (zeitlich beschränkt auf die Identitätskontrolle) und die interne IHK-Prüfungsorganisation (nach finaler Notenfreigabe) einsehbar.
  - *Getrennte Verarbeitung der Nachteilsausgleichsparameter*: Die Umsetzungsparameter nach Ziff. 5.3 werden in einem eigenen, gesondert verschlüsselten Datenbereich mit eigenem Rollenprofil geführt; jeder Lesezugriff wird protokolliert. Prüferoberflächen und Korrekturmasken haben auf diesen Bereich keinen Zugriff.
- **Nichtverkettung**: \* *Multi-Tenancy*: Konsequente logische Trennung aller Datenströme nach der IHK-Mandanten-ID. Datenbankabfragen über mehrere Mandanten hinweg sind applikationsseitig technisch ausgeschlossen.
- **Transparenz**: \* *Fachlicher Audit Trail*: Revisionssicheres, nicht manipulierbares Logging aller bewertungsrelevanten Aktionen (z. B. manuelle Notenänderungen durch Prüfer oder Schreibzeitverlängerungen durch Aufsichten).
- **Intervenierbarkeit**: \* *Echtzeit-Steuerung*: Funktionen für Aufsichten, um Prüfungen bei individuellen Störungen zu pausieren, abubrechen oder auf Ersatzgeräte umzuziehen.
  - *Sperr-Flags*: Ermöglichung der manuellen Aussetzung automatischer Löschrufen bei schwebenden Widerspruchsverfahren.

### 11.3 Ebene 3: Technische Infrastruktur (Infrastruktur- und Hosterbezogene Maßnahmen)

- **Vertraulichkeit**: \* *Data at Rest*: Vollständige Festplattenverschlüsselung (AES-256) aller Produktiv- und Backup-Systeme.
  - *Data in Transit*: Durchgängige Verschlüsselung aller Übertragungswege mittels TLS 1.3 unter Nutzung sicherer Cipher Suites sowie mTLS für die interne Server-zu-Server-Kommunikation.
- **Integrität**: \* *Confidential VMs*: Nach Möglichkeit Einsatz von Confidential-Computing-Technologien zur Verschlüsselung von Daten im Arbeitsspeicher der Server.

- *Zentraler Logserver*: Weiterleitung aller Infrastruktur-Logs in Echtzeit an einen dedizierten, schreibgeschützten SIEM-Server außerhalb der administrativen Zugriffsebene des Produktivhosters.
- **Verfügbarkeit**: \* *Georedundanz*: Täglich automatisierte Backups, die georedundant in mindestens zwei physisch getrennten, zertifizierten Rechenzentren (Mindestabstand nach BSI-Vorgaben) gelagert werden.
  - *Recovery-Testing*: Vierteljährliche, automatisierte Wiederherstellungstests zur Verifikation der Wiederanlaufzeiten (RTO/RPO).
- **Datenminimierung**: \* *Sicheres Löschen*: Physische Vernichtung ausgedienter Datenträger nach BSI-konformen Standards; sicheres Überschreiben freigegebener Cloud-Speichersektoren.
  - *Log-Rotation*: Automatische Löschung technischer Webserver-Logs (wie IP-Adressen) nach maximal 7 Tagen.
- **Nichtverkettung**: \* *Kryptografische Schematrennung*: Verwendung isolierter Datenbankschemata mit separaten Schlüsseln je IHK-Mandant.
- **Transparenz**: \* *Echtzeit-Monitoring*: Kontinuierliche Überwachung der Infrastruktur durch ein automatisiertes Security Operations Center (SOC).
- **Intervenierbarkeit**: \* *Selective Backup Shredding*: Technische Fähigkeit, bei berechtigten Löschbegehren einzelne Datensätze gezielt aus bestehenden Backup-Archiven zu entfernen („shreddern“), ohne die Gesamtintegrität des Backups zu gefährden.

## 12. Schnittstellen und Datenflüsse

### 12.1 Schnittstellen-Governance auf drei Ebenen

Der Datenaustausch mit angebundenen Systemen (wie EVA, Tibros oder ADELE) unterliegt strengen Sicherheits- und Abgrenzungsregeln:

- **Ebene 1 (Fachverfahren)**: Die einspeisenden Stellen (regionale IHKs und Aufgabenerstellungseinrichtungen) tragen die alleinige Verantwortung für die Richtigkeit und rechtliche Zulässigkeit der exportierten Daten. Sie müssen prozessual sicherstellen, dass nur Daten importiert werden, die für das aktuelle Prüfungsfenster zwingend erforderlich sind.
- **Ebene 2 (Fachapplikation)**: Alle APIs müssen als *Tenant-Aware APIs* konzipiert sein. Ein API-Aufruf (z. B. zur Notenübermittlung an ADELE) ist hardcodiert an den Authentifizierungstoken des jeweiligen IHK-Mandanten gekoppelt. Ein mandantenübergreifender Datenabruf über eine Schnittstelle ist technisch unmöglich. Alle eingehenden Daten werden automatisiert auf Formatkonformität und Schadcode geprüft; fehlerhafte Datenpakete werden sofort abgewiesen und protokolliert.
- **Ebene 3 (Technische Infrastruktur)**: Schnittstellenaufrufe sind ausschließlich über verschlüsselte Kommunikationskanäle (TLS 1.3) zulässig. Die Authentifizierung erfolgt über starke, zeitlich begrenzte Tokens oder zertifikatsbasierte API-Keys, die auf autorisierte

Quell-IP-Adressen der IHK-Rechenzentren beschränkt sind (*Zero-Trust-API*).

## 13. Exit-Strategie und Datenlöschung

Zur Vermeidung eines *Vendor Lock-in* und zur Gewährleistung der dauerhaften Datenhoheit der IHKs wird eine datenschutzkonforme Exit-Strategie vertraglich und technisch festgeschrieben:

### 13.1 Interoperabler Datenexport (Ebene 2)

Der Plattformanbieter ist verpflichtet, im Exit-Fall alle personenbezogenen Daten (Stammdaten, Prüfungsergebnisse, Protokolle, Audit-Trails) in einem strukturierten, gängigen und maschinenlesbaren Format (**JSON oder XML**) bereitzustellen. Zusammen mit den Daten ist das vollständige, detaillierte Datenbankschema (*Data Dictionary*) in deutscher Sprache zu übergeben.

### 13.2 Das zweistufige Exit-Löschverfahren

1. Nach erfolgreicher Übergabe der Exportdateien an die IHKs werden die Daten auf der Plattform für jeglichen regulären Zugriff gesperrt (**Stufe 1: Sperrung**).
2. Eine endgültige, physische Löschung darf erst nach Ablauf einer Bestätigungs- und Karenzzeit von **90 Tagen** erfolgen. Die Löschung wird erst durchgeführt, wenn die empfangenden IHKs den fehlerfreien Import und die Validität der Daten im Nachfolgesystem schriftlich oder in Textform bestätigt haben.
3. Der Anbieter muss die unwiderrufliche Löschung (BSI-konformes Überschreiben der Datenträger) auf allen Produktiv- und Backup-Systemen durch ein qualifiziertes, mandantenbezogenes Löschprotokoll nachweisen (**Stufe 2: Physische Löschung**).
4. Die Unterstützung des Anbieters bei der Datenmigration im Rahmen des Exits (Bereitstellung von APIs, Formatklärungen) ist wesentlicher Bestandteil der vertraglichen Leistungspflicht und darf nicht durch prohibitive Sonderhonorare blockiert werden.

## 14. Einsatz von Systemen mit Künstlicher Intelligenz (KI-Systeme)

Sollten im Rahmen der Prüfungsplattform KI-gestützte Funktionen (z. B. zur automatisierten Vorbewertung von Freitextaufgaben oder zur KI-gestützten Prüfungsüberwachung) zum Einsatz kommen, gelten im Jahr 2026 die strengen Bestimmungen der **Verordnung (EU) 2024/1689 (europäische KI-Verordnung / AI Act)** sowie der DSGVO:

### 14.1 Absolute Ausschlusskriterien und verbotene KI-Praktiken (Art. 5 KI-Verordnung)

Der Einsatz folgender KI-Praktiken ist auf der Plattform technisch und organisatorisch **absolut**

**ausgeschlossen und verboten:**

- **Emotionserkennung im Prüfungskontext (Art. 5 Abs. 1 lit. f KI-Verordnung):** Jede Form von KI-Systemen, die darauf abzielt, die emotionalen Zustände von Prüflingen während der Prüfung (z. B. durch Mimik- oder Verhaltensanalyse im Rahmen einer Videoüberwachung) zu erkennen, zu bewerten oder zu protokollieren, ist im Bildungs- und Prüfungsbereich strengstens verboten.
- **Biometrische Kategorisierung und Social Scoring:** Systeme, die natürliche Personen auf Basis biometrischer Daten sensiblen Kategorien zuordnen oder deren Verhalten bewerten, sind unzulässig.

## **14.2 Restriktionen für Hochrisiko-KI-Systeme (Anhang III & Art. 6 KI-Verordnung)**

KI-Systeme, die im Bildungs- und Berufsbildungsbereich zur Bewertung von Prüfungsleistungen oder zur Überwachung von Prüflingen eingesetzt werden, fallen grundsätzlich in die Kategorie der **Hochrisiko-KI-Systeme**. Ihr Einsatz ist auf der Plattform grundsätzlich ausgeschlossen.

Ein Einsatz solcher Systeme ist ausnahmsweise **nur unter folgenden kumulativen Bedingungen zulässig:**

1. **Ausnahmeregelung nach Art. 6 Abs. 3 KI-Verordnung:** Es wird nachgewiesen, dass das System kein erhebliches Risiko für die Grundrechte natürlicher Personen birgt, weil es lediglich eine **rein unterstützende oder vorbereitende Teiltätigkeit** (z. B. strukturelle Vor-Sortierung von Freitexten ohne Notenvorschlag) ausführt.
2. **Umfassende Compliance:** Die strengen Anforderungen des Kapitels 2 der KI-Verordnung (Risikomanagement, Daten-Governance, technische Dokumentation, automatisiertes Logging und menschliche Aufsicht) werden nachweislich erfüllt.
3. **Spezifisches Betriebskonzept:** Ein detailliertes Betriebskonzept für den konkreten KI-Einsatz wurde ausgearbeitet, durch die Datenschutzbeauftragten geprüft und **durch die Geschäftsführung der jeweils betroffenen regionalen IHK explizit freigegeben**.

## **14.3 Technische Gewährleistung der KI-Datenschutzziele**

- **Integrität (Bias-Minimierung & Halluzinationsschutz):** Der Auftragnehmer muss nachweisen, dass die zum Training der KI genutzten Datensätze repräsentativ und frei von systemischen Verzerrungen (Bias) bezüglich Herkunft, Sprache oder Behinderungen sind. Bei generativen Modellen müssen Validierungsmechanismen (z. B. *Retrieval-Augmented Generation* - RAG) vorgeschaltet werden, um "Halluzinationen" unzutreffender Fakten technisch auszuschließen.
- **Intervenierbarkeit (Recht auf menschliche Überprüfung - Human-in-the-Loop):** Eine rein automatisierte Einzelfallentscheidung (Art. 22 DSGVO) ohne menschliche Bewertung ist rechtlich unzulässig. Die Applikation (Ebene 2) muss eine zwingende Workflow-

Schranke enthalten: Jedes KI-vorbereitete Ergebnis muss dem zuständigen menschlichen Prüfungsausschuss zur finalen Prüfung, Abänderung und manuellen Freigabe vorgelegt werden. Die Letztentscheidungskompetenz verbleibt vollständig beim Menschen.

- **Transparenz (Kennzeichnungspflicht nach Art. 50 KI-Verordnung):** Prüflingen ist vor Prüfungsbeginn in leicht verständlicher Weise offenzulegen, wenn ein KI-System im Prozess zum Einsatz kommt. Die KI muss in der Lage sein, ihre Bewertungsvorschläge anhand der hinterlegten Musterlösungen transparent und nachvollziehbar zu begründen (*Explainable AI*).

## 14.4 Mandantenbezogenes Steuerungskonzept (Opt-In / Opt-Out)

Es darf keine plattformweite, pauschale Aktivierung von KI-Funktionen geben.

- **Tenant-Level Control (Ebene 2):** Jeder IHK-Mandant muss angebotene KI-Funktionen unabhängig aktivieren (*Opt-In*) oder vollständig deaktivieren (*Opt-Out*) können.
- **Strikte Kapselung (Ebene 3):** Ist eine KI-Funktion für einen Mandanten deaktiviert, ist technisch sicherzustellen, dass keinerlei Prüfungs- oder Stammdaten dieses Mandanten an die KI-Infrastruktur oder zugehörige APIs übertragen werden.
- **Striktes Trainingsverbot:** Die Nutzung personenbezogener Daten von Prüflingen oder Prüfern zum Zwecke des Trainings, des Finetunings oder der Weiterentwicklung der KI-Modelle des Plattformbetreibers oder von Drittanbietern ist **strikt untersagt**.

## 15. Governance und Weiterentwicklung

Der Lenkungskreis beauftragt das Projektteam im Rahmen der in der Leistungsbeschreibung genannten Maßnahmen und Entscheidungsbefugnisse mit der kontinuierlichen Überwachung der datenschutzrechtlichen Compliance der Plattform.

### 15.1 Das Change Advisory Board (CAB)

Zur datenschutzkonformen Weiterentwicklung der Plattform wird ein **Change Advisory Board (CAB)** eingerichtet:

- Der Plattformanbieter muss geplante funktionale Änderungen (Ebene 2) vorab dem CAB vorlegen.
- Das CAB bewertet die Auswirkungen auf den Datenschutz (*Privacy by Design*).
- Bei wesentlichen Änderungen erstellt die DIHK unter Mitwirkung des Anbieters eine **zentrale Aktualisierung der Muster-DSFA** und stellt diese den IHKs zur Verfügung. Ein neues Feature wird erst dann für den jeweiligen IHK-Mandanten freigeschaltet, wenn die IHK die aktualisierte DSFA lokal übernommen hat.

### 15.2 Kontinuierliche Evaluierung (Audits und Pentests)

- **Regelmäßige Penetrationstests:** Alle zwei Jahre, sowie vor jedem Major-Release, ist die Plattform (Ebene 2 und 3) durch einen unabhängigen, zertifizierten IT-

Sicherheitsdienstleister umfassenden technischen Penetrationstests zu unterziehen.

- **Zentralisiertes Audit-Verfahren (Art. 28 Abs. 3 lit. h DSGVO):** Die regionalen IHKs bevollmächtigen den Lenkungskreis, einmal jährlich ein gemeinsames, umfassendes Audit (Datenschutz- und Sicherheitsprüfung) beim Plattformanbieter und dessen Rechenzentren durch einen unabhängigen Prüfer durchführen zu lassen. Der detaillierte Bericht wird allen IHKs zur Verfügung gestellt, um redundante und kostspielige Einzel-Vor-Ort-Prüfungen zu vermeiden.