DKS GmbH (Anlage 2)
Datenschutz gemäß Art. 32 DSGVO
Technische und organisatorische Maßnahmen

Kontrollziele bezüglich Umgang mit personenbezogenen Daten	**Maßnahmen**
1. **Zugangskontrolle** (Räume und Gebäude) Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte	**Bereich mit Eingangskontrolle** • Beim DKS Servicebetrieb in München handelt es sich um einen Closed-Shop-Betrieb. Der Zutritt ist nur Mitarbeitern im Rahmen ihrer Tätigkeit gestattet. Zutritt zu den Räumlichkeiten der DKS GmbH erhalten Besucher ausschließlich in Begleitung von Firmenangehörigen. Datenschutzzonen mit Zugangs-berechtigung innerhalb des Closed-Shop-Betriebes. • Protokollierung der Zu- und Abgänge.
2. **Datenträgerkontrolle** Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern	• Absicherung der Bereiche, in denen Datenträger aufbewahrt werden (Datenträgerarchiv, Safe) • Aufbewahrung im ext. Gebäude • Maßnahmen gegen unbefugtes Entfernen von Datenträgern • Protokollierung der autorisierten Weitergabe von Datenträgern • Datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger

Kontrollziele bezüglich Umgang mit personenbezogenen Daten	**Maßnahmen**
3. **Speicherkontrolle** Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten	• Einsatz von Mitteln zur Identifikation und Authentisierung der Benutzer • revisionsfähige Zugriffsberechtigungs-verwaltung • Softwareverriegelung des Bildschirmes bei längerem Inaktivsein des Benutzers • Trennung des Test- und Produktionsbetriebes • Kontrolle der System- und User-Aktivitäten (z. B. Protokollierung der Art des Datenzugriffs) • Datenverschlüsselung
4. **Benutzerkontrolle** Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte	• Festlegung der nutzungsberechtigten Personen • Identifikation und Authentifizierung der Benutzer • Sicherung der Datenstationen • Verschlüsselung der zu übertragenden Daten • Protokollierung der Benutzer und deren Aktivitäten

Kontrollziele bezüglich Umgang mit personenbezogenen Daten	**Maßnahmen**
5. **Zugriffskontrolle** Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben	• Anlage von revisionsfähigen Benutzerprofilen • Identifikation und Authentifizierung der Benutzer • Maschinelle Überprüfung der Berechtigungen • Einführung zugriffsbeschränkender Maßnahmen (z. B. nur Leseberechtigung) • Benutzerbezogene Protokollierung der (Fehl-)Zugriffe • Einsatz von Verschlüsselungsverfahren Die Zugriffskonzepte, sowohl innerhalb der Anwendung als auch auf Basis des Betriebssystems, folgen dem „Prinzip der Minimalen Rechte“. Mitarbeitern werden nur die zur Durchführung ihrer Tätigkeit notwendigen Rollen und Rechte zugewiesen, sämtliche Logins sind personalisiert. • **DKS Portal:** Die Übertragung der Daten wird vollständig verschlüsselt auf Basis eines RSA Public-/Privat Key Exchange und AES (256 Bit) Session Encoding durchgeführt. • Die Dokumente und Benutzer-passwörter sind mittels AES Session Encoding (256 Bit) Verschlüsselung in der DKS Portal Datenbank gegen unberechtigte Einsichtnahme geschützt. • Fehlerhafte Anmeldeversuche am DKS Portal werden überwacht und in der Datenbank entsprechend protokolliert.
6. **Übertragungskontrolle** Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können	• Dokumentation der Abruf- und Übermittlungsprogramme • Festlegung der Übertragungswege und der Datenempfänger • Protokollierung der Datenübertragung • Auswertungsmöglichkeiten der Übermittlungsprotokolle, um die Empfänger oder Abrufenden gezielt feststellen zu können

Kontrollziele bezüglich Umgang mit personenbezogenen Daten	**Maßnahmen**
7. **Eingabekontrolle** Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind	Im DKS Vollservice-Betrieb • Festlegung von Eingabebefugnissen • Kontrolle der Eingaben, Veränderungen und Löschungen im 4-Augen-Prinzip Datenverarbeitung durch den Auftraggeber • Eingabekontrolle wird ausschließlich durch den Kunden umgesetzt
8. **Transportkontrolle** Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden	• Festlegung der für die Übermittlung oder den Transport Berechtigten • Regelungen für die Versandart und Festlegung des Transportweges • Sicherung des Übertragungs- und Transportweges • Verschlüsselung der Daten auf dem Transportweg

Kontrollziele bezüglich Umgang mit personenbezogenen Daten	**Maßnahmen**
9. **Wiederherstellbarkeit** Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können	• Regelmäßige Datensicherung • Tägliches backup der Systeme. Die Aufbewahrung erfolgt Gebäude getrennt im feuersicheren Datensicherheits-schrank. • Für das DKS Portal gelten die TOM für managed Systeme des Unter-auftragnehmers PlusServer GmbH. Es erfolgt ebenso ein tägliches backup.
10. **Zuverlässigkeit** Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden	• Regelmäßiges update der OS • Firewall • Virenschutz der Server- und Clientsysteme Das Serversystem ist mit redundanten Festplatten ausgerüstet. Tägliches Backup, offsite-Backup, Virenscan-Routinen und regelmäßige Sicherheits- und Funktions-Updates gewährleisten die Verfügbarkeit der Daten. Zusätzlich werden Sicherungen auf externe Datenträger durchgeführt. • Für das DKS Portal gelten die TOM für managed Systeme des Unter-auftragnehmers PlusServer GmbH.

Kontrollziele bezüglich Umgang mit personenbezogenen Daten	**Maßnahmen**
11. **Datenintegrität** Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können	• Jährliche Zertifizierung durch ITSG Die Daten werden bei der Erfassung maschinell auf Zulässigkeit, Vollständigkeit und Richtigkeit geprüft. Fehlerhaft erkannte Daten werden protokolliert und nicht in die Entgeltunterlagen übernommen.
12. **Auftragskontrolle** Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können	• Klare Vertragsgestaltung und -ausführung • Abgrenzung der Kompetenzen und Pflichten zwischen Auftragnehmer und Auftraggeber • Sorgfältige Auswahl des Unterauftragnehmers • Formalisierung der Auftragserteilung • Protokollierung und Kontrolle der ordnungsgemäßen Vertragsausführung Personenbezogene Daten werden nur gemäß den Weisungen des Auftraggebers verarbeitet. Grundlage hierfür bilden der Dienstleistungsvertrag und das Abwicklungsstammblatt, die zwischen der DKS Daten-Kontroll-Systeme GmbH und dem Auftraggeber vereinbart wurden.

Kontrollziele bezüglich Umgang mit personenbezogenen Daten	**Maßnahmen**
13. **Verfügbarkeitskontrolle** Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind	• Das Serversystem im Rechenzentrum ist mit redundanten Festplatten ausgerüstet. Zusätzlich werden Sicherungen auf externe Datenträger durchgeführt. Die Aufbewahrung erfolgt Gebäude getrennt im feuersicheren Datensicherheitsschrank. • Für das DKS Portal gelten die TOM für managed Systeme des Unter-auftragnehmers PlusServer GmbH.
14. **Trennbarkeit** Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können	• Mandantenfähige Datenbanksysteme • Allgemein - bitte beachten Sie dazu unsere Ausführungen zum Zugriff.