

# Vereinbarung

zwischen

---

Name und Anschrift

---

Ansprechpartner

- Verantwortlicher - nachstehend Auftraggeber genannt -

und

**KÜS DATA GmbH, Zur KÜS 1, 66679 Losheim am See**

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

## 1. Gegenstand und Dauer des Auftrags

### (1) Gegenstand

Gegenstand des Auftrags ist die Verarbeitung von Bilddateien von Fahrzeugscheinen (Zulassungsbescheinigung Teil 1). Im Einzelnen werden Fahrzeugscheine mittels einer speziellen Texterkennung (KI OCR) ausgelesen. Die dabei entstehenden Daten werden nach dem Ausleseprozess per Textdatei (JavaScript Object Notation) an den Auftraggeber übermittelt. Unmittelbar nach der Verarbeitung werden sowohl die Bilddateien, als auch die Textdateien gelöscht.

Zum Gegenstand des Auftrags zählt nicht die Nutzung personenbezogener Daten des Auftraggebers durch den Auftragnehmer. Ein Zugriff auf die personenbezogenen Daten des Auftraggebers im Zuge des Supports oder der Administration von Server-Systemen kann jedoch nicht ausgeschlossen werden.

### (2) Dauer

Die Dauer des Auftrags (Laufzeit) entspricht der Laufzeit des Nutzungsvertrags.

## 2. Konkretisierung des Auftragsinhalts

### (1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Der Auftraggeber übermittelt dem Auftragnehmer Bilddateien einer Zulassungsbescheinigung Teil 1. Die Serversysteme des Auftragnehmers lesen mittels OCR-Texterkennung verschiedene Felder aus der Zulassungsbescheinigung aus und übermitteln die Ergebnisse im Textformat zurück an den Auftraggeber. Die ausgelesenen Felder können sowohl personenbezogene, als auch nicht personenbezogene Daten enthalten.

Zum Zwecke der Vertragserfüllung kann ein Zugriff des Auftragnehmers auf die unter Punkt 2 aufgeführten Daten nicht ausgeschlossen werden.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

### (2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten können folgende Datenarten/-kategorien sein:

- Personenstammdaten (Halterdaten)
- Fahrzeugidentifikationsnummer (FIN)
- KFZ-Kennzeichen
- weitere nicht personenbezogene Daten zum jeweiligen Fahrzeug

### (3) Kategorien betroffener Personen

Die Kategorien, der durch die Verarbeitung möglicherweise betroffenen Personen umfassen:

- Kunden

## 3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen, um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen [Einzelheiten siehe ToM in Anlage].

(2) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

(3) Der Auftragnehmer dokumentiert die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung. Der Auftragnehmer ermöglicht und unterstützt die Prüfung der Umsetzung der vereinbarten Maßnahmen vor Beginn, sowie während der Verarbeitung durch die Auftraggeberin.

## 4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

## 5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt. Dessen aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt unter <https://www.kues-data.de/datenschutz/>.
- b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten des Auftraggebers haben könnten, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
- c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO [Einzelheiten siehe ToM in Anlage].
- d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
- f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
- g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
- h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

## 6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

- Eine Unterbeauftragung erfolgt derzeit nicht.
- Die Auslagerung auf Unterauftragnehmer oder
- der Wechsel des bestehenden Unterauftragnehmers zulässig sind, soweit:
  - der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
  - der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
  - eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer ist nicht gestattet.

Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

## 7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO.
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO.
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren).
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI-Grundschutz).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch

geltend machen.

## 8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u. a.:

- a) Die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen.
- b) Die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden.
- c) Die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen.
- d) Die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung.
- e) Die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

## 9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

## 10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber - spätestens mit Beendigung der Leistungsvereinbarung - hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

### **Anlagen**

Die folgenden Anlagen sind Bestandteile dieser Vereinbarung:

- Anlage 1: Technisch-organisatorische Maßnahmen zur Einhaltung des Datenschutzes

\_\_\_\_\_  
Ort, Datum

\_\_\_\_\_  
Ort, Datum

\_\_\_\_\_  
Auftraggeber

\_\_\_\_\_  
Auftragnehmer, KÜS DATA GmbH

# Maßnahmen zur Sicherstellung der Vertraulichkeit und Integrität gem. Art. 32 Abs.1 b) DSGVO

## Zutrittskontrolle

### *Prof.-Pirlet-Straße 27-29 - KÜS DATA Rechenzentrum*

Der Standort ist in vier ineinander liegende Sicherheitsbereiche aufgeteilt. Diese werden über ein elektronisches Zutrittskontrollsystem gesteuert.

Tagsüber überwacht eigenes Personal und in der Nacht überwacht ein externer Wachdienst den Zutritt des Gebäudes. Der Zutritt in die Sicherheitsbereiche wird nur für autorisierte Personen gewährleistet. Videokameras sowie Einbruchmelder überwachen die Außenhaut des Gebäudes. Im Alarmfall werden die verantwortlichen Mitarbeiter, ein örtlicher Wachdienst und eine externe Wachzentrale alarmiert.

Das Gebäude ist gemäß DIN EN 50600 VK 3 SK 1-4 zertifiziert.

Die Identität von Besuchern wird am Empfang mittels Ausweisdokument kontrolliert. An- und Abmeldung von Besuchern werden elektronisch protokolliert. Besucher müssen sich mittels Besucherausweis im Gelände ausweisen. Es besteht eine restriktive Zutrittsregelung.

Kundensysteme befinden sich in sog. abgeschlossenen Racks. Diese sind alarmgesichert und müssen vor dem Öffnen von der Zentrale freigegeben werden.

### *Zur KÜS 1*

Der Zutritt wird über ein elektronisches Zutrittskontrollsystem gesteuert. Tagsüber überwacht eigenes Personal und in der Nacht überwacht ein externer Wachdienst den Zutritt des Gebäudes. Der Zutritt in die Sicherheitsbereiche wird nur für autorisierte Personen gewährleistet. Videokameras sowie Einbruchmelder überwachen die Außenhaut des Gebäudes. Im Alarmfall werden die verantwortlichen Mitarbeiter, ein örtlicher Wachdienst und eine externe Wachzentrale alarmiert. Es besteht eine restriktive Zutrittsregelung.

## Zugangskontrolle

### *Allgemein KÜS-Verbund*

Alle Systeme sind mit einem Passwortschutz versehen. Die Komplexität und der Umgang mit Passwörtern sind in der Passworrichtlinie geregelt. Die Benutzerkontrolle erfolgt mittels Active-Directory-Authentifizierung.

Zugang zu Servern, Netzwerk- und Sicherheitseinrichtungen haben nur wenige autorisierte Personen.

Externe Zugänge (VPN) sind über eine Zwei-Faktorauthentifizierung gesichert. Netzwerkzugangspunkte werden über restriktive Firewallregeln mit UTM-Funktion abgesichert.

### *gemanagte Kundensysteme im KÜS DATA Rechenzentrum*

Zugang zu Systemen haben nur wenige autorisierte Personen, sowie der Kunde selbst.

Alle Systeme sind mit einem Passwortschutz versehen. Die Komplexität und der Umgang mit Passwörtern sind in der Passworrichtlinie geregelt.

### ***nicht gemanagte Kunden-Systeme im KÜS DATA Rechenzentrum***

Auf kundeneigene Systeme hat die KÜS DATA keinen Zugriff. Es obliegt dem Kunden die Systeme abzusichern. Ggfs. kann der Kunde einen Firewalldienst bei uns hinzubuchen.

## **Zugriffskontrolle**

### ***Allgemein KÜS-Verbund***

Schreib- und Lesezugriffsberechtigungen sind personenbezogen und werden über Sicherheitsgruppen im MS Active-Directory realisiert. Auf Daten die nicht dem Active-Directory-Berechtigungskonzept unterliegen haben nur wenige autorisierte Personen Zugriff, dies wird über die Zugangskontrolle sichergestellt.

Berechtigungsänderungen werden nur von der Geschäftsführer- und Leitungsebene vorgenommen oder an einen berechtigten Administrator delegiert. Berechtigungsänderungen werden dokumentiert.

### ***gemanagte Kundensysteme im KÜS DATA Rechenzentrum***

Auf die Daten haben nur wenige autorisierte und für die Systeme verantwortliche Personen Zugriff.

### ***nicht gemanagte Kunden-Systeme im KÜS DATA Rechenzentrum***

Der Kunde ist selbst für eine Zugriffsregelung verantwortlich. Die KÜS DATA hat keinen Zugriff auf die Systeme.

## **Trennungskontrolle**

### ***Allgemein KÜS-Verbund***

Daten werden Zwecks ihrer Erhebung auf unterschiedlichen Systemen aufbewahrt. Die zweckmäßige Verarbeitung ist über das Berechtigungskonzept gewährleistet.

### ***gemanagte Kundensysteme im KÜS DATA Rechenzentrum***

Kundensysteme laufen zum Teil auf derselben Hardware. Die Systeme sind Mandantenfähig und durch Sicherheitsmechanismen logisch voneinander getrennt, z. B. durch VLAN, Sandboxing etc.

## **Weitergabekontrolle**

### ***Allgemein KÜS-Verbund***

Eine technisch notwendige Zugriffsmöglichkeit auf alle übertragenen Daten besteht im Rahmen der Verwaltung der Netzwerkhardware (Router, Switches). Dieser Zugriff ist auf die Mitarbeiter der Administration beschränkt und dient ausschließlich zur Gewährleistung des technischen Betriebes.

Die Übermittlung von personenbezogenen Daten wird nur von geschultem Personal durchgeführt und den Übermittlungsstandards entsprechend gesichert.

Nicht mehr benötigte Datenträger werden fachmännisch zerstört und von einem Fachunternehmen zur Datenträgerbeseitigung entsorgt.



## Eingabekontrolle

### *Allgemein KÜS-Verbund*

Wie unter dem Punkt „Vertraulichkeit“ beschrieben haben alle Benutzer eigene Benutzerzugänge. An- und Abmeldungen werden von dem jeweiligen System in einer Logdatei protokolliert. Die Logdateien werden gemäß der jeweiligen Aufbewahrungsfrist aufbewahrt.

### *nicht gemanagte Kunden-Systeme im KÜS DATA Rechenzentrum*

Der Kunde ist selbst für die Protokollierung seiner Systeme zuständig. Die KÜS hat keinen Zugriff auf die Systeme.

## Maßnahmen zur Sicherstellung der Verfügbarkeit und Belastbarkeit der Systeme gem. Art. 32 Abs.1 b) DSGVO

## Verfügbarkeitskontrolle

### *Allgemein KÜS-Verbund*

Um die Verfügbarkeit zu gewährleisten betreibt der KÜS-Verbund seine IT-Infrastruktur im DIN EN 50600 VK 3 SK 1-4 zertifiziertem Rechenzentrum der KÜS DATA.

Alle Daten werden nach ihrem jeweiligen Schutzbedarf zusätzlich von einem Backup-System nach Stand der Technik in einem örtlich getrennten Brandabschnitt gesichert.

Hardware die den Betrieb gewährleistet ist redundant als Active-/Active- oder Active-/Passive-Cluster ausgelegt.

### *gemanagte Kundensysteme im KÜS DATA Rechenzentrum*

Alle Systeme stehen im DIN EN 50600 VK 3 SK 1-4 zertifiziertem Rechenzentrum der KÜS DATA.

Hardware die den Betrieb gewährleistet ist redundant als Active-/Active- oder Active-/Passive-Cluster ausgelegt. Je nach Produkt ist ein definierter Backup-Zeitraum für die Daten enthalten oder der Kunde kann eine regelmäßige Sicherung hinzubuchen.

### *nicht gemanagte Kunden-Systeme im KÜS DATA Rechenzentrum*

Die KÜS DATA stellt die DIN EN 50600 VK 3 SK 1-4 zertifizierte Gebäudeinfrastruktur des Rechenzentrum zur Verfügung.

Für den Betrieb der kundeneigenen Hardware ist der Kunde zuständig. Ggfs. kann der Kunde ein Backup-Produkt der KÜS DATA einsetzen.

## Wiederherstellbarkeit

### Allgemein KÜS-Verbund

Die Daten im KÜS-Verbund werden von einem Backup-System gesichert. Bei Datenverlust lassen sich die Daten mittels Instand Recovery in wenigen Minuten wiederherstellen.

Die KÜS DATA unterhält mit verschiedenen Hardwarelieferanten Supportverträge welche bei Hardwaredefekten eine Ersatzteillieferung innerhalb weniger Stunden garantiert.

## Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung gem. Art. 32 Abs.1 d) DSGVO

### Datenschutz-Management

Der KÜS-Verbund unterhält ein umfassendes Datenschutz-Management. Hierzu hat er eine Unternehmensrichtlinie zum Schutz personenbezogener Daten erstellt, in der beschrieben ist, welche Arten von personenbezogenen Daten erhoben, wie diese Daten genutzt, an wen sie übermittelt werden und welche Wahlmöglichkeiten und Rechte betroffene Personen im Zusammenhang mit der Verarbeitung ihrer Daten haben. Außerdem wird dort beschrieben, mit welchen Maßnahmen die Sicherheit der Daten gewährleistet wird und wie betroffene Personen Kontakt mit dem KÜS-Verbund aufnehmen können, wenn Sie Fragen zur Datenschutzpraxis haben. Die Richtlinie regelt darüber hinaus die datenschutzkonforme Informationsverarbeitung und die insoweit bei der KÜS und ihren verbundenen Unternehmen bestehenden Verantwortlichkeiten.

### Incident-response-Management

Um auf mögliche Datensicherheitsverletzungen, DoS (Denial of Service), DDoS (Distributed Denial of Service), Lücken in der Firewall, Ausbrüche von Viren oder Malware und auch Bedrohungen durch Insider schnellstmöglich reagieren zu können, gibt es Vorfallreaktionspläne mit Anweisungen, auf welche Weise die zuständigen Personen auf potenzielle Szenarios reagieren sollten.

### Auftragskontrolle

Eine Verarbeitung personenbezogener Daten im Auftrag des KÜS-Verbunds werden gemäß Art. 28 DSGVO nur auf eindeutige Weisung und nach strenger Auswahl des Dienstleisters zugelassen. Hierzu gehört u. a. eine eindeutige Vertragsgestaltung, ein formalisiertes Auftragsmanagement und die Möglichkeit von Nachkontrollen.