Vereinbarung

über die Verarbeitung personenbezogener Daten

zwischen

.....

.....

.....

- Verantwortlicher - nachstehend Auftraggeber genannt -

und

Gebrauchtwagenheld GmbH
Trakehner Straße 7b
60487 Frankfurt am Main

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt -

Diese Vereinbarung garantiert dem Auftraggeber in Übereinstimmung mit Art. 28 Abs. 1 DSGVO, dass eine Verarbeitung personenbezogener Daten in dessen Auftrag durch die Autengo GmbH ausschließlich auf Grund geeigneter technischer und organisatorischer Maßnahmen so durchgeführt wird, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

I. Gegenstand und Dauer der Vereinbarung

1. Gegenstand

Diese Vereinbarung findet Anwendung auf alle Tätigkeiten, die in unseren Allgemeinen Geschäftsbedingungen (AGB) sowie in unserem Hauptvertrag aufgeführt sind, sofern im Rahmen dieser Tätigkeiten personenbezogene Daten verarbeitet werden.

Hierzu gehört insbesondere die Speicherung personenbezogener Daten durch unsere Kunden (Autohändler) im Rahmen unserer Verwaltungssoftware.

Ferner fallen hierunter, der Remotezugriff auf den Account unserer Händler durch unsere Mitarbeiter im Zusammenhang mit Supportanfragen.

2. Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

Der Auftraggeber kann die Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in dieser Vereinbarung vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

II. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen

Zweck der Verarbeitung von personenbezogenen Daten durch uns als den Auftragnehmer ist es, dem Auftraggeber eine übersichtliche digitale Akte zur Verfügung zu stellen, mit deren Hilfe er seine Waren, sowie Kunden, Interessenten und Lieferanten und die dazugehörige Kommunikation mit diesen Personengruppen verwalten kann.

Von der Datenverarbeitung betroffene Personen gemäß Definition von Art. 4 Nr. 1 DS-GVO sind damit:

- □ Kunden
- □ Interessenten
- □ Beschäftigte
- □ Lieferanten

des Auftraggebers (Autohändlers).

Von den oben genannten Personengruppen werden folgende Datenarten verarbeitet:

- □ Personenstammdaten
- □ Kommunikationsdaten (z.B. Telefon, E-Mail)
- □ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- □ Kundenhistorie (bisherige Fahrzeuge, Vorlieben in Bezug auf Fahrzeuge etc.)
- □ Vertragsabrechnungs- und Zahlungsdaten
- □ Planungs- und Steuerungsdaten
- □ Sowie alle Daten, die der Auftraggeber bei der Nutzung der Software in das frei ausfüllbare Notizfeld einträgt.

Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

III. Rechte und Pflichten des Auftraggebers

1. Verantwortlichkeit des Auftraggebers

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen ist allein der Auftraggeber verantwortlich.

Der Auftraggeber hat den Auftragnehmer von Ansprüchen Dritter aufgrund angeblich unrechtmäßigen Datenverarbeitungen freizustellen soweit jene auf Fahrlässigkeit oder Vorsatz des Auftraggebers beruhen.

2. *Kontrollrecht des Auftraggebers*

Der Auftraggeber ist berechtigt, sich vor Beginn der Verarbeitung und sodann regelmäßig jährlich in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in dieser Vereinbarung festgelegten Verpflichtungen zu überzeugen.

Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

3. Pflicht der Vertraulichkeit

Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieser Vereinbarung bestehen.

IV. Weisungsbefugnisse des Auftraggebers

Dem Auftraggeber bleibt ein Weisungsrecht vorbehalten.

Hierdurch entstehende Mehrkosten sind vom Auftraggeber zu erstatten.

Dem Auftragnehmer bleibt das Recht vorbehalten, solche Weisungen zu verweigern, die eine erhebliche Steigerung des Arbeitsaufwands zur Folge hätten.

Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich. Mündliche Weisungen sind unverzüglich schriftlich zu bestätigen.

V. Rechte und Pflichten des Auftragnehmers

1. Pflicht der weisungsgebundenen Verarbeitung

Der Auftragnehmer verarbeitet die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation –, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

Der Auftragnehmer informiert den Auftraggeber unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen diese Verordnung oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

2. Recht auf Aussetzung der Weisung

Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

3. Vertraulichkeits- / Verschwiegenheitspflicht

Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

4. Maßnahmen zur Gewährleistung von Sicherheit und Ordnung

Der Auftragnehmer gewährleistet, unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.
Dies beinhaltet insbesondere:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten.
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen.
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Eine ausführliche Darstellung der technischen und organisatorischen Maßnahmen wird dieser Vereinbarung als Anlage beigefügt.

5. *Pflicht der Unterstützung des Auftraggebers bei der Erfüllung seiner gesetzlichen Pflichten*

Der Auftragnehmer gewährleistet, den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten des Auftraggebers und bei der Erfüllung der Rechte der betroffenen Personen aus Kapitel III der DSGVO beziehungsweise nach Art. 12 bis 22 DS-GVO, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers im notwendigen Umfang und angesichts der Art der Verarbeitung den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen angemessen zu unterstützen. Soweit dem Auftragnehmer hierdurch Aufwand und Kosten entstehen, sind diese vom Auftraggeber zu erstatten.

6. *Mitteilungspflichten des Auftragnehmers bei Störung der Verarbeitung und bei Verletzung des Schutzes personenbezogener Daten*

Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DSGVO.

7. *Löschungs- und Rückgabepflicht*

Der Auftragnehmer gewährleistet, nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder zu löschen oder zurückzugeben und die vorhandenen Kopien zu löschen, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Die Modalitäten der Löschung und Rückgabe legt der Auftraggeber vertraglich oder durch Weisung fest. Hieraus resultierende Zusatzkosten sind vom Auftraggeber zu tragen.
Gleiches gilt für durch den Auftraggeber überlassene und damit grundsätzlich im Eigentum desselbigen gebliebene Datenträger sowie sämtliche hiervon gefertigte Kopien und Reproduktionen.

8. *Kontrollpflichten*

Der Auftragnehmer wird die Erfüllung seiner Pflichten kontrollieren und dokumentieren.

Der Auftragnehmer gewährleistet, dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in dieser Vereinbarung niedergelegten Pflichten zur Verfügung zu stellen und Überprüfungen – einschließlich Inspektionen –, die - grundsätzlich nach Terminvereinbarung - vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, zu ermöglichen und dazu beizutragen.

9. *Informationspflichten*

Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Auffassung ist, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

10. *Pflicht der Weiterleitung von an den Auftraggeber gerichteten Anfragen*

Der Auftragnehmer ist verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

VI. Unterbeauftragung

Der Auftraggeber erklärt sich damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner Leistungspflichten die in der Anlage benannten weiteren Auftragsverarbeiter beauftragt.
Der Auftragnehmer informiert den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

Der Auftragnehmer wird den weiteren Auftragsverarbeitern im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegen, die in dem Vertrag oder anderen Rechtsinstrument zwischen dem Auftraggeber und dem Auftragnehmer festgelegt sind.
Es werden insbesondere hinreichende Garantien dafür geboten, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt. Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters.

VII. Schlussbestimmungen

1. Diese Vereinbarung und deren Anlagen können im Fall der Änderung datenschutzrechtlicher Bestimmungen angepasst werden.

2. Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform.

3. Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam sein, bleibt die Wirksamkeit dieser Vereinbarung davon im Übrigen unberührt.

Anlage 1 – Liste der beauftragten Subunternehmer

AWS Webservices

a) Name und Anschrift des Dienstleisters

Amazon Web Services, Inc.
410 Terry Avenue North
Seattle WA 98109
United States

Amazon Web Services, Inc. ist eine nach dem Recht des Staates Delaware gegründete und registrierte Gesellschaft.
Registernummer: 4152954, Secretary of State, State of Delaware.
Steuernr.: 204938068

Vertretungsberechtigter: Associate General Counsel, EMEA

aws.amazon.com
Fax: +1 206 266-7010
AWS Kontakt

b) Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen:

Amazon Web Services ist ein US-amerikanischer Cloud-Computing Anbieter. Da wir in unseren Räumlichkeiten über keine eigenen Server zum Speichern unser Daten verfügen, werden alle Inhalte unserer Software auf den Servern von Amazon Web Services gespeichert. Diese Daten werden jedoch nur auf Servern der Amazon Web Services Inc. Gespeichert, die in Frankfurt am Main in Deutschland lokalisiert sind.

Damit werden folgende Datenarten und Datenkategorien von Amazon Web Services in unseren Auftrag verarbeitet.

Von der Datenverarbeitung betroffene Personen gemäß Definition von Art. 4 Nr. 1 DS-GVO sind damit:

- □ Kunden
- □ Interessenten
- □ Beschäftigte
- □ Lieferanten

des Auftraggebers (Autohändlers).

Von den oben genannten Personengruppen werden folgende Datenarten verarbeitet:

- □ Personenstammdaten
- □ Kommunikationsdaten (z.B. Telefon, E-Mail)
- □ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- □ Kundenhistorie (bisherige Fahrzeuge, Vorlieben in Bezug auf Fahrzeuge etc.)
- □ Vertragsabrechnungs- und Zahlungsdaten
- □ Planungs- und Steuerungsdaten

Technische und organisatorische Maßnahmen i.S.d. Art. 32 DSGVO betreffend Softwareleistungen

der

Gebrauchtwagenheld GmbH
Trakehner Straße 7 B
60487 Frankfurt am Main

---

1. Zutrittskontrolle

Maßnahmen, die verhindern, dass Unbefugte Zutritt zu Gebäuden und Räumen bekommen in denen sich Datenverarbeitungsanlagen befinden, mit denen personenbezogene Daten verarbeitet oder genutzt werden.

- ☐ Alarmanlage
- ☐ Automatisches Zugangskontrollsystem
- ☐ Schließsystem mit Codesperre
- ☐ Biometrische Zugangssperren
- ☐ Lichtschranken / Bewegungsmelder
- ☑ Schlüsselregelung (Schlüsselausgabe etc.)
- ☐ Protokollierung der Besucher
- ☐ Sorgfältige Auswahl von Wachpersonal
- ☐ Absicherung von Gebäudeschächten
- ☑ Chipkarten-/Transponder-Schließsystem
- ☐ Manuelles Schließsystem
- ☑ Videoüberwachung der Zugänge
- ☑ Sicherheitsschlösser
- ☐ Personenkontrolle beim Pförtner / Empfang
- ☑ Sorgfältige Auswahl von Reinigungspersonal
- ☐ Tragepflicht von Berechtigungsausweisen

2. Zugangskontrolle

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

- ☑ Zuordnung von Benutzerrechten
- ☑ Passwortvergabe
- ☑ Authentifikation mit Benutzername / Passwort
- ☐ Gehäuseverriegelungen
- ☐ Sperren von externen Schnittstellen (USB etc.)
- ☑ Einsatz von Antivirus Software
- ☐ Protokollierung der Besucher
- ☐ Einsatz von Intrusion-Detection-Systemen
- ☑ Restriktive Vergabe von Adminrechten auf Clients
- ☐ Einsatz von Anti-Viren-Software
- ☑ Erstellen von Benutzerprofilen
- ☐ Authentifikation mit biometrischen Verfahren
- ☑ Zuordnung von Benutzerprofilen zu IT-Systemen
- ☑ Einsatz von VPN-Technologie
- ☐ Tragepflicht von Berechtigungsausweisen
- ☑ Passwortrichtlinie zur Änderung, Komplexität und Geheimhaltung
- ☑ Mitarbeiterschulung
- ☐ Verschlüsselung von mobilen Datenträgern
- ☐ Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)
- ☐ Verschlüsselung von Datenträgern in Laptops / Notebooks

☐ Einsatz einer Hardware-Firewall

☑ Einsatz einer Software-Firewall

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.

☑ Erstellen eines Berechtigungskonzepts

☑ Verwaltung der Rechte durch Systemadministrator

☑ Anzahl der Administratoren auf das „Notwendigste“ reduziert

☑ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel

☑ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten

☑ Sichere Aufbewahrung von Datenträgern

☐ physische Löschung von Datenträgern vor Wiederverwendung

☑ ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)

☑ Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)

☐ Protokollierung der Vernichtung

☑ Verschlüsselung von Datenträgern

4. 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

☐ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form

☐ E-Mail-Verschlüsselung

☐ Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen

☐ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen

☐ Beim physischen Transport: sichere Transportbehälter/-verpackungen

☑ Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und –fahrzeugen

5. Eingabekontrolle

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

- ☐ Protokollierung der Eingabe, Änderung und Löschung von Daten
- ☑ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- ☑ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- ☑ Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
- ☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind

6. Auftragskontrolle

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

- ☑ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- ☑ schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag) i.S.d. Art. 28 DSGVO
- ☑ Auftragnehmer hat Datenschutzbeauftragten bestellt
- ☑ Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
- ☐ Vertragsstrafen bei Verstößen
- ☑ vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
- ☑ Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
- ☑ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- ☑ laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten

7. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt und für den Verantwortlichen stets verfügbar sind.

- ☑ Unterbrechungsfreie Stromversorgung (USV)
- ☑ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- ☑ Feuer- und Rauchmeldeanlagen
- ☐ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- ☑ Testen von Datenwiederherstellung
- ☑ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- ☑ Klimaanlage in Serverräumen
- ☑ Schutzsteckdosenleisten in Serverräumen
- ☑ Feuerlöschgeräte in Serverräumen
- ☑ Erstellen eines Backup- & Recoverykonzepts
- ☐ Erstellen eines Notfallplans
- ☐ Serverräume nicht unter sanitären Anlagen

☐ In Hochwassergebieten: Serverräume über der Wassergrenze

8. Trennungsgebot

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

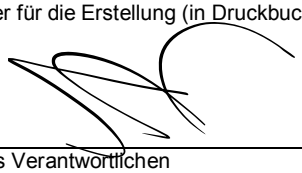
- ☑ physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- ☑ Erstellung eines Berechtigungskonzepts
- ☐ Versehen der Datensätze mit Zweckattributen/Datenfeldern
- ☑ Festlegung von Datenbankrechten
- ☐ Logische Mandantentrennung (softwareseitig)
- ☐ Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- ☐ Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System
- ☑ Trennung von Produktiv- und Testsystem

9. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit technisch-organisatorischer Maßnahmen

- ☐ Penetrationstests
- ☑ Verpflichtung der Mitarbeiter auf das Datengeheimnis
- ☑ Mitarbeiter sind angehalten nicht mehr personenbezogene Daten zu erheben als für den jeweiligen Zweck erforderlich
- ☑ Firewall, Virenscanner und Spamfilter werden eingesetzt und regelmäßig aktualisiert
- ☑ Mitarbeiter erhalten Weisung zum Umgang mit personenbezogenen Daten

24.05.2018
Datum

Sebastian Fischer
Verantwortlicher für die Erstellung (in Druckbuchstaben)



Unterschrift des Verantwortlichen