1. Vertraulichkeit	***Vertraulichkeit als Teil der Informationssicherheit - Es sollen geeignete Maßnahmen sicherstellen, dass Informationen nur einem bestimmten Empfängerkreis zugänglich sind, wie z.B. Verpflichtung Verschluss, Verschlüsselung, Passwortregel, Kontrolle, Zertifizierung.***
Zutrittskontrolle:	*Maßnahmen, damit Unbefugten der Zutritt zu den Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogene Daten verarbeitet werden.* - Das Gebäude ist mit einer Schließanlage gesichert - Es existiert ein manuelles Schließsystem mit Sicherheitsschlössern - Die Nutzung der Schließanlage ist dokumentiert - Zutritt von Dritten nur mit Voranmeldung (Türklingel) - Der Zutritt und Aufenthalt von Besuchern erfolgt in Begleitung von Firmenpersonal - Protokollierung von Besuchern - Der Zutritt von Reinigungs- und Wartungspersonal zum Gebäude ist geregelt - Die Reinigung erfolgt durch Personal, das auf das Datengeheimnis verpflichtet ist und nur eingeschränkten Zugang zu datenschutzrelevanten Bereichen hat.
Zugangskontrolle:	*Maßnahmen, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und Datenverarbeitungsverfahren benutzen.* - Alle Rechner verfügen über individuelle, personenbezogene Benutzerkennungen - Es existiert eine Protokollierung der Benutzeranmeldung - Es existiert eine Passwortrichtlinie (16 Zeichen, Großbuchstaben, Kleinbuchstaben, Sonderzeichen, Ziffern) - Eine automatisierte Sperrung bei Inaktivität der Rechner ist vorhanden - Das Firmennetzwerk ist durch eine Firewall und Virenschutz geschützt - Der Zugang von außen auf das Netzwerk wird durch verschlüsselte Verbindungen sichergestellt (SSL und HTTPS) - Zwei-Faktor-Authentisierung wird eingesetzt, sofern sie systemseitig angeboten wird.
Zugriffskontrolle:	*Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können.* - Ein Berechtigungskonzept ist systemseitig vorhanden - Die Verwaltung der Rechte erfolgt nur durch Systemadministratoren - Nur vereinzelte mit besonderen Aufgaben versehene Mitarbeiter haben Administrationsrechte - Der Einsatz von Aktenvernichter/Schredder ist gewährleistet - Sorgfältige Auswahl der Mitarbeiter - Zugriff erfolgt nur nach konkreter Beauftragung durch den Auftraggeber über das Ticketsystem des Auftragnehmers - Arbeiten erfolgen nur im Rahmen dessen, was zur Lösung des vom Auftraggeber geschilderten Problems notwendig ist - Weitergehende Arbeiten erfolgen nur in Abstimmung mit dem Auftraggeber - Daten auf Festplatten, welche endgültig aus einem Server entfernt werden, werden umgehend, dauerhaft und unwiederbringlich entfernt

Trennungsgebot:	*Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können*. - Der Auftragnehmer nutzt personenbezogene Daten nur für interne Zwecke im Rahmen des Auftrages oder der Kundenbeziehung - Eine physische oder (programm-)technische Trennung von Daten (Mandantentrennung) ist vorhanden - Es existiert eine Festlegung von Datenbankrechten - Auf unterschiedliche Kundenumgebungen kann nur mit unterschiedlichen Identifizierungen zugegriffen werden - Alle Mitarbeiter sind angewiesen und geschult, Daten nur im Rahmen der Leistungserbringung und zur Wahrung der Zweckbindung zu erheben, zu verarbeiten und zu nutzen - Eine Trennung von Produktiv- und Testsystem ist vorhanden
Anonymisierung / Pseudonymisierung:	*Die Anonymisierung ist das Verändern personenbezogener Daten derart, dass diese Daten nicht mehr einer Person zugeordnet werden können. Bei der Pseudonymisierung wird der Name oder ein anderes Identifikationsmerkmal durch ein Pseudonym ersetzt, um die Feststellung der Identität des Betroffenen auszuschließen oder wesentlich zu erschweren.* - Bei Fernwartung und anderen Supporttätigkeiten werden Daten eingesehen. Es findet keine weitere Verarbeitung statt. Die Daten werden nicht weitergegeben. Deshalb finden Maßnahmen wie Pseudonymisierung und Anonymisierung keine Anwendung.
Im Falle von Bereitstellung von IT-Infrastruktur / Hosting:	*Maßnahmen, die die Vertraulichkeit im Falle von Bereitstellung von IT-Infrastruktur / Hosting auf einem (oder mehreren) dedizierten Server(n) sowie der damit im Zusammenhang stehenden Leistungen sicherstellen:* Wartungsarbeiten (Support) im Rahmen von Migration, Serverzugriff zur Anpassung und Fehlerbehebung sowie Systempflege finden außerhalb der Räumlichkeiten des Auftraggebers statt. Eine Überwachung der Wartungsarbeiten ist daher nur eingeschränkt möglich. Der Serverzugriff durch den Auftragnehmer erfolgt mittels VPN-Verbindung direkt ins Rechenzentrum des Auftragnehmers. Der Zugriff durch den Auftragnehmer auf die Administrationsoberfläche erfolgt per Webbrowser mittels sicherer SSL-Verbindung. Findet Support am Arbeitsplatzrechner eines Mitarbeiters des Auftraggebers statt (Vor-Ort-Wartung oder mittels Fernwartungssoftware), muss der Mitarbeiter des Auftragnehmers während der Wartungsarbeiten durch einen Mitarbeiter des Auftraggebers beaufsichtigt werden. Wartungsarbeiten finden nach vorheriger Absprache zwischen Auftraggeber und Auftragnehmer statt. Darin eingeschlossen sind Arbeiten im Rahmen einer Migration und Serverzugriff zur Anpassung und Fehlerbehebung. Die durchgeführten Wartungsarbeiten werden durch Rückmeldung des Ergebnisses an den Auftraggeber protokolliert (Die Kommunikation mit dem Auftraggeber erfolgt über das CRM-System des Auftragnehmers). Die Abstimmung erfolgt projektbezogen in Abstimmung zwischen Auftraggeber und Auftragnehmer oder fallbezogen über ein Support-Ticket. Wartungsarbeiten zur Systempflege (Serverperformance, Festplattenkapazität …) finden ohne vorherige Absprache statt. Durch diese Arbeiten wird ein reibungsloser Betrieb der Anwendung sichergestellt. Im Rahmen dieser Arbeiten erfolgt kein Zugriff auf Datenbestände der Anwendung.

2. Integrität	***Integrität als Teil der Informationssicherheit – Es sollen geeignete Maßnahmen sicherstellen, dass die Korrektheit bzw. Unversehrtheit von Daten und die korrekte Funktionsweise von Systemen gewährleistet wird, wie z.B. Zugriffsbeschränkung, Prüfsummen, Fehleranalyse.***
Eingabekontrolle:	*Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind.* - Auf den Systemen des Auftragnehmers ist die Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) gegeben - Die Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten erfolgt auf Basis eines Berechtigungskonzepts - Zugriff erfolgt nur nach konkreter Beauftragung durch den Auftraggeber über das Ticketsystem des Auftragnehmers - Bearbeitender Mitarbeiter auf Seiten des Auftragnehmers ist durch eine persönliche Benutzerkennung im Ticketsystem identifizierbar
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.* - Eine Weitergabe von personenbezogenen Daten ist nicht Bestandteil des Auftrages.
3. Verfügbarkeit	***Verfügbarkeit als Teil der Informationssicherheit – Geeignete Maßnahmen sollen sicherstellen, dass IT-Systeme innerhalb der erwarteten Zeit die an sie gestellten Anforderungen erfüllen. Dazu gehören u.a. Infrastrukturmaßnahmen, System-Wartung, Datensicherung.***
	- Die Aufbewahrung der Datensicherung findet an einem sicheren, ausgelagerten Ort statt - Der Zugang zu Storage-Lösungen wird für Unbefugte physisch verhindert - Alle Speichersysteme verfügen über eine interne Festplattenspiegelung - Datenträger und Datenspeicher werden zugriffssicher aufbewahrt
4. Belastbarkeit	***Der Begriff der Belastbarkeit („Resilienz") beschreibt die Fähigkeit des Unternehmens, auch bei Störungen und Eingriffen möglichst unbeschadet weiter existieren zu können.***
	- Ein Patch Management ist vorhanden - Datenträger und Datenspeicher unterliegen einem Aufbewahrungs- und Löschkonzept
5. Wiederherstellung	***Es sollen Maßnahmen beschrieben werden die sicherstellen, dass nach einem IT-Systemausfall in angemessener Zeit die Funktionsfähigkeit wiederhergestellt werden kann. Stehen Kontaktdaten der Systembetreuer, Hard- und Software und aktuelle Daten zur Verfügung?***

	- Ein Datensicherheitskonzept ist vorhanden - Aktuelle Backuplösungen zur Wiederherstellbarkeit sind vorhanden - Eine kurze Wiederanlaufzeit der Server ist durch eine vorhandene Redundanz gewährleistet - Der sichere Lebenszyklus von Datenträgern ist geregelt
6. Evaluierung	***Welche dokumentierten Regelungen gibt es, damit der Stand der Informationssicherheit regelmäßig geprüft und aktualisiert wird? Werden Prüfungen durchgeführt, ausgewertet und die zu treffenden Maßnahmen kontrolliert?***
	- Ein Datenschutzbeauftragter wurde für das Unternehmen bestellt - Gemäß Art. 35, Abs. 4 DS-GVO ist für die durchgeführte Verarbeitung keine Datenschutz-Folgenabschätzungen notwendig - Alle Mitarbeiter mit Zugriff auf personenbezogenen Daten sind auf „Vertraulichkeit der Daten“ verpflichtet - Jährliche Hinweise und Ermahnungen, um das Problembewusstsein zu fördern, finden per vor-Ort-Termin oder als Videokonferenz statt, zuletzt am 1. Dezember 2025. - Ein Prozess für das Auskunftsverfahren Betroffener ist eingerichtet - Ein Incident-Managementsystem ist vorhanden - Es finden gelegentliche unvermutete Kontrolle der Einhaltung von Datenschutz- und Datensicherungsmaßnahmen statt - Ein Datenschutzmanagement ist vorhanden

17. Februar 2026	*Johannes Kaut*	
geprüft am (Datum)	*geprüft von (Name)*	*Unterschrift (Datenschutzkoordinator)*

Unsere externe Datenschutzbeauftragte hat die technischen und organisatorischen Maßnahmen (TOM) geprüft und bestätigt hiermit die Einhaltung der in diesem Dokument genannten Maßnahmen. Die TOM werden mindestens einmal im Jahr einer kompletten Prüfung unterzogen und aktuelle technische Entwicklungen und organisatorische Änderungen einbezogen. Rückblickend auf die vergangenen 36 Monate gab es keine Datenpannen bei der DocHouse GmbH.

Signature: 

17. Februar 2026	*Ulrike Eben*	**Email:** ulrike.eben@danubis.net
geprüft am (Datum)	*geprüft von (Name)*	*Unterschrift (Datenschutzbeauftragte)*

Die Richtigkeit der Angaben wird bestätigt durch die Geschäftsleitung der DocHouse GmbH.

Signature: 

17. Februar 2026	*Wolfgang Brugger*	**Email:** wolfgang.brugger@dochouse.de
geprüft am (Datum)	*geprüft von (Name)*	*Unterschrift (Geschäftsführer)*

TOM

Final Audit Report 2026-02-18

Created:	2026-02-17
By:	Johannes Kaut (johannes.kaut@dochouse.de)
Status:	Signed
Transaction ID:	CBJCHBCAABAAQo3EfahUf-wxDHIJ6ayct0dfyRUIaq7D

"TOM" History

Document created by Johannes Kaut (johannes.kaut@dochouse.de)
2026-02-17 - 1:04:41 PM GMT- IP address: 62.246.35.11

Document emailed to Ulrike Eben (ulrike.eben@danubis.net) for signature
2026-02-17 - 1:04:45 PM GMT

Email viewed by Ulrike Eben (ulrike.eben@danubis.net)
2026-02-18 - 7:41:28 AM GMT- IP address: 217.241.226.5

Document e-signed by Ulrike Eben (ulrike.eben@danubis.net)
Signature Date: 2026-02-18 - 7:42:35 AM GMT - Time Source: server- IP address: 217.241.226.5

Document emailed to Wolfgang Brugger (wolfgang.brugger@dochouse.de) for signature
2026-02-18 - 7:42:37 AM GMT

Email viewed by Wolfgang Brugger (wolfgang.brugger@dochouse.de)
2026-02-18 - 7:53:49 AM GMT- IP address: 95.222.30.65

Document e-signed by Wolfgang Brugger (wolfgang.brugger@dochouse.de)
Signature Date: 2026-02-18 - 7:56:18 AM GMT - Time Source: server- IP address: 95.222.30.65

Agreement completed.
2026-02-18 - 7:56:18 AM GMT