# Anlage 1 – Technische und organisatorische Maßnahmen (TOMs)

Chatline • Stand: März 2026

Die nachfolgenden technischen und organisatorischen Maßnahmen dienen der Gewährleistung eines dem Risiko angemessenen Schutzniveaus gemäß Art. 32 DSGVO. Sie beziehen sich auf die Verarbeitung personenbezogener Daten im Rahmen der Bereitstellung und des Betriebs von Chatline.

Die Maßnahmen werden unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen umgesetzt und fortlaufend weiterentwickelt.

## 1. Organisation, Verantwortlichkeiten und Datenschutzmanagement

1. HeyHo Systems unterhält organisatorische Prozesse zur datenschutzkonformen und sicheren Verarbeitung personenbezogener Daten.
2. Zuständigkeiten für Datenschutz, Informationssicherheit, Entwicklung, Betrieb und Support sind intern festgelegt.
3. Mitarbeitende und sonstige berechtigte Personen werden auf Vertraulichkeit verpflichtet und in angemessenem Umfang zu Datenschutz- und Sicherheitsanforderungen sensibilisiert.
4. Interne Prozesse für den Umgang mit Sicherheitsvorfällen, Betroffenenanfragen, Supportzugriffen, Berechtigungen und Löschanforderungen sind eingerichtet.
5. Änderungen an Systemen, Konfigurationen und produktiven Funktionen erfolgen kontrolliert und nachvollziehbar.

## 2. Zutrittskontrolle

6. Der physische Zutritt zu IT-Systemen und Infrastruktur, auf denen personenbezogene Daten verarbeitet werden, ist auf berechtigte Personen beschränkt.
7. Soweit Infrastruktur durch externe Hosting- oder Cloud-Anbieter betrieben wird, erfolgt die physische Absicherung durch deren Rechenzentrums- und Sicherheitskonzepte.
8. Interne Arbeitsmittel werden gegen unbefugten Zugriff geschützt, insbesondere durch Gerätepasswörter, Bildschirmsperren und organisatorische Vorgaben.

## 3. Zugangs- und Authentifizierungskontrolle

9. Der Zugriff auf produktive Systeme erfolgt nur für berechtigte Personen.
10. Zugänge werden individuell vergeben und sind personenbeziehbar.
11. Es bestehen Verfahren zur sicheren Verwaltung von Zugangsdaten und Geheimnissen.
12. Für administrative oder besonders schutzrelevante Zugriffe werden angemessene zusätzliche Sicherungsmaßnahmen eingesetzt, insbesondere starke Passwörter, rollenbezogene Berechtigungen und, soweit vorgesehen, Mehrfaktor-Authentifizierung.

13. Nicht mehr erforderliche Zugänge werden deaktiviert oder entfernt.

## 4. Zugriffskontrolle und Berechtigungskonzept

14. Der Zugriff auf personenbezogene Daten ist nach dem Need-to-know-Prinzip und entsprechend der jeweiligen Rolle beschränkt.
15. Berechtigungen werden nur insoweit vergeben, als sie für die jeweilige Aufgabe erforderlich sind.
16. Administrative, betriebliche, Entwicklungs- und Supportzugriffe werden funktional getrennt, soweit dies technisch und organisatorisch sinnvoll ist.
17. Zugriffe auf produktive Daten erfolgen nur, soweit dies für Betrieb, Support, Fehleranalyse, Sicherheit oder die Umsetzung dokumentierter Weisungen erforderlich ist.
18. Berechtigungen werden bei Bedarf überprüft und angepasst.

## 5. Weitergabe- und Übertragungskontrolle

19. Personenbezogene Daten werden bei elektronischer Übertragung nach dem Stand der Technik gegen unbefugten Zugriff geschützt, insbesondere durch Transportverschlüsselung.
20. Externe Zugriffe auf Systeme und Schnittstellen erfolgen über abgesicherte Kommunikationswege.
21. Datenübermittlungen an Dienstleister und Unterauftragnehmer erfolgen nur im erforderlichen Umfang und auf vertraglicher Grundlage.
22. Soweit eine Übermittlung in Drittländer erfolgt, werden die gesetzlichen Anforderungen des Kapitels V DSGVO eingehalten.

## 6. Eingabekontrolle und Nachvollziehbarkeit

23. Wesentliche Systemereignisse, Betriebszustände und technische Fehler können protokolliert werden, soweit dies für Sicherheit, Stabilität, Missbrauchserkennung, Fehleranalyse oder Nachvollziehbarkeit erforderlich ist.
24. Soweit technisch vorgesehen, können administrative Änderungen, Supportzugriffe oder sicherheitsrelevante Vorgänge nachvollzogen werden.
25. Protokolle werden gegen unberechtigten Zugriff geschützt und nur im erforderlichen Umfang ausgewertet.
26. Protokollierungsdaten werden nicht zu vertragsfremden Zwecken verwendet.

## 7. Auftragskontrolle

27. Personenbezogene Daten werden ausschließlich im Rahmen der vertraglichen Vereinbarungen und dokumentierten Weisungen des Auftraggebers verarbeitet, soweit keine gesetzliche Verpflichtung entgegensteht.
28. Interne Prozesse stellen sicher, dass Verarbeitungen nicht eigenmächtig zu anderen Zwecken erfolgen.
29. Eine Nutzung personenbezogener Daten des Auftraggebers für eigenes Marketing sowie für das Training oder die Weiterentwicklung eigener oder fremder KI-Modelle mit personenbezogenen Daten des Auftraggebers ist ausgeschlossen.
30. Unterauftragnehmer werden nur nach Maßgabe der vertraglichen Regelungen eingebunden und vertraglich datenschutzgerecht verpflichtet.

## 8. Verfügbarkeitskontrolle und Belastbarkeit

31. Systeme und Dienste werden so betrieben, dass eine angemessene Verfügbarkeit und Belastbarkeit gewährleistet ist.
32. Es bestehen Maßnahmen zur Erkennung und Behandlung technischer Störungen und Betriebsunterbrechungen.
33. Soweit erforderlich, werden Datensicherungen, Redundanzen, Wiederherstellungs- oder Notfallmechanismen eingesetzt.
34. Sicherungskopien und Wiederherstellungsprozesse werden organisatorisch und technisch geschützt.
35. Die Wirksamkeit von Verfügbarkeits- und Wiederherstellungsmaßnahmen wird in angemessenem Umfang überprüft.

## 9. Trennungskontrolle

36. Personenbezogene Daten verschiedener Auftraggeber werden logisch voneinander getrennt verarbeitet, soweit mehrere Mandanten auf derselben technischen Plattform betrieben werden.
37. Test-, Entwicklungs- und Produktivumgebungen werden organisatorisch und soweit möglich technisch voneinander getrennt.
38. Der Einsatz produktiver personenbezogener Daten in Test- oder Entwicklungsumgebungen erfolgt nur, soweit dies ausnahmsweise erforderlich, angemessen abgesichert und datenschutzrechtlich zulässig ist.
39. Daten werden zweckgebunden verarbeitet und nicht ohne rechtliche Grundlage oder Weisung in andere Verarbeitungskontexte überführt.

## 10. Pseudonymisierung, Datenminimierung und Speicherbegrenzung

40. Personenbezogene Daten werden nur in dem Umfang verarbeitet, der für die vertraglich vorgesehenen Zwecke erforderlich ist.
41. Soweit technisch, organisatorisch und wirtschaftlich sinnvoll, werden Maßnahmen zur Reduzierung des Personenbezugs eingesetzt, etwa durch Begrenzung von Datenfeldern, Rollenbeschränkungen, selektive Sichtbarkeit, Löschroutinen oder vergleichbare Mechanismen.
42. Für verarbeitete Daten bestehen Aufbewahrungs- und Löschprozesse oder Löschkonzepte.
43. Daten werden gelöscht, anonymisiert oder in der Verarbeitung beschränkt, sobald sie für die Zwecke der Verarbeitung nicht mehr erforderlich sind und keine gesetzlichen oder berechtigten Aufbewahrungsgründe entgegenstehen.
44. Löschungen in Backups erfolgen im Rahmen der regulären Sicherungs- und Rotationsprozesse.

## 11. Integrität und Schutz vor unbefugter Veränderung

45. Es bestehen technische und organisatorische Maßnahmen, um personenbezogene Daten vor unbefugter oder unbeabsichtigter Veränderung zu schützen.
46. Änderungen an produktiven Systemen erfolgen kontrolliert und nachvollziehbar.
47. Konfigurationen, Geheimnisse und sicherheitsrelevante Parameter werden vor unbefugtem Zugriff und unzulässiger Änderung geschützt.

## 12. Verschlüsselung und Geheimnisschutz

48. Datenübertragungen erfolgen über abgesicherte Verbindungen.
49. Soweit angemessen und vorgesehen, werden gespeicherte Daten oder besonders schutzbedürftige Geheimnisse verschlüsselt oder durch gleichwertige Maßnahmen geschützt.
50. Zugangsschlüssel, Tokens, API-Credentials und vergleichbare Geheimnisse werden gesondert geschützt und nur berechtigten Stellen zugänglich gemacht.
51. Geheimnisse werden bei Bedarf rotiert, ersetzt oder entzogen.

## 13. Entwicklung, Deployment und Änderungsmanagement

52. Änderungen an Anwendungen, Schnittstellen und Infrastruktur erfolgen über definierte Entwicklungs- und Deployment-Prozesse.
53. Neue Funktionen, Integrationen und Änderungen werden vor produktiver Nutzung in angemessenem Umfang geprüft.
54. Sicherheitsrelevante Änderungen und Fehlerbehebungen werden priorisiert behandelt.
55. Quellcode, Konfigurationen und Build-/Deployment-Prozesse werden gegen unbefugten Zugriff geschützt.

## 14. Support- und Wartungszugriffe

56. Support- und Wartungszugriffe auf personenbezogene Daten erfolgen nur, soweit dies für Fehleranalyse, Support, Wartung, Sicherheitsmaßnahmen oder die Umsetzung dokumentierter Weisungen erforderlich ist.
57. Solche Zugriffe sind auf berechtigte Personen beschränkt.
58. Soweit technisch vorgesehen, können Supportzugriffe dokumentiert oder nachvollzogen werden.
59. Daten aus Support- oder Wartungskontexten werden nicht für eigene Zwecke verwendet.

## 15. Umgang mit Sicherheitsvorfällen und Datenschutzverletzungen

60. Es bestehen organisatorische Prozesse zur Erkennung, Bewertung, Behandlung und Nachverfolgung von Sicherheitsvorfällen.
61. Verletzungen des Schutzes personenbezogener Daten werden intern geprüft, dokumentiert und – soweit erforderlich – dem Auftraggeber unverzüglich mitgeteilt.
62. Der Auftragnehmer trifft angemessene Maßnahmen zur Eindämmung, Untersuchung und Behebung von Vorfällen.
63. Erkenntnisse aus Vorfällen fließen in die Weiterentwicklung von Schutzmaßnahmen ein.

## 16. Regelmäßige Überprüfung und Weiterentwicklung

64. Die technischen und organisatorischen Maßnahmen werden in angemessenem Umfang regelmäßig überprüft und bei Bedarf angepasst.
65. Änderungen der technischen Infrastruktur, der Bedrohungslage, der eingesetzten Dienstleister oder der Produktfunktionalitäten können Anlass für eine Anpassung der TOMs sein.
66. Das Schutzniveau wird dabei insgesamt nicht wesentlich abgesenkt.

## 17. Besondere Maßnahmen im Zusammenhang mit KI-, Sprach- und Kommunikationsdiensten

67. Chatline nutzt technische Dienste für Kommunikationsübermittlung, Sprachverarbeitung sowie KI-gestützte Inhaltsverarbeitung.
68. Die Einbindung solcher Dienste erfolgt nur, soweit dies für die vertragliche Leistungserbringung erforderlich ist.
69. Soweit personenbezogene Daten an solche Dienste übermittelt werden, erfolgt dies auf vertraglicher Grundlage und im erforderlichen Umfang.
70. Eine Verwendung personenbezogener Daten des Auftraggebers zum Training eigener oder fremder Modelle außerhalb der vertraglich geschuldeten Leistung ist ausgeschlossen.
71. Es werden keine Anrufaufzeichnungen gespeichert; soweit Sprachinhalte verarbeitet werden, erfolgt dies grundsätzlich zum Zweck der Erstellung von Transkripten, Gesprächssteuerung, Zusammenfassungen oder der Bearbeitung des jeweiligen Anliegens.

## 18. Homeoffice und mobile Arbeit

72. Soweit berechtigte Personen im Homeoffice oder mobil arbeiten, gelten angemessene organisatorische und technische Sicherheitsanforderungen.
73. Dazu gehören insbesondere der Schutz von Endgeräten, abgesicherte Zugänge, Bildschirmsperren sowie der Schutz vor Einsichtnahme durch unberechtigte Dritte.
74. Personenbezogene Daten sollen außerhalb kontrollierter Systemumgebungen nur verarbeitet werden, soweit dies erforderlich und angemessen abgesichert ist.

## 19. Unterauftragnehmer

75. Unterauftragnehmer werden sorgfältig ausgewählt und nur eingesetzt, soweit sie hinreichende Garantien für eine datenschutzgerechte Verarbeitung bieten.
76. Mit Unterauftragnehmern werden vertragliche Regelungen geschlossen, die ein angemessenes Datenschutzniveau sicherstellen.
77. HeyHo Systems überwacht Unterauftragnehmer im angemessenen Umfang durch vertragliche, organisatorische oder dokumentarische Maßnahmen.
78. Die jeweils aktuellen Unterauftragnehmer werden in einer gesonderten Subprozessorenliste dokumentiert.