TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN GEMÄSS DSG/DSV

Das vorliegende Dokument bietet eine Übersicht über die technischen und organisatorischen Massnahmen des Datenschutzes (TOM) der Health Info Net AG. Die gesetzlichen Pflichten ergeben sich aus dem Schweizerischen Bundesgesetz über den Datenschutz (DSG) sowie der dazugehörigen Verordnung (DSV), insbesondere aus den Art. 7 und 8 DSG und Art. 3 DSV.

Die Massnahmen decken den normalen und hohen Schutzbedarf ab und betreffen Personendaten sowie besonders schützenswerte Personendaten. Falls durch die Bearbeitung von besonders schützenswerten Personendaten nach Umsetzung der TOM weitere Risiken bestehen, so wird eine Risikobeurteilung durchgeführt, um zu bestimmen, welche zusätzliche Massnahmen zu ergreifen sind.

In der folgenden Tabelle sind die Anforderungen aus der Verordnung über den Datenschutz, die jeweiligen Massnahmen seitens HIN und die entsprechenden Anforderungen der Zertifizierung gemäss ISO/IEC 27001 aufgeführt. Diese Tabelle dient Kunden von HIN – in Ergänzung zur Datenschutzerklärung und den Rahmenverträgen – als Nachweis für die getroffenen Massnahmen; ebenso in der Beziehung zwischen HIN und ihren Lieferanten, weshalb in Auftragsbearbeitungsvereinbarungen (ABV) mit Lieferanten darauf verwiesen wird.

DSV Art. 3	Kurzbeschreibung und Umsetzung bei HIN	Referenzierte Anforderungen ISO/IEC 27001:2017[1]	Referenzierte Anforderungen ISO/IEC 27001:2022[2]
1 Um die **Vertraulichkeit** zu gewährleisten, müssen der **Verantwortliche** und der **Auftragsbearbeiter** geeignete Massnahmen treffen, damit: a. berechtigte Personen nur auf diejenigen Personendaten Zugriff haben, die sie zur Erfüllung ihrer Aufgaben benötigen (**Zugriffskontrolle**);	Zugriffskontrolle umfasst organisatorische und technische Massnahmen um sicherzustellen, dass nur authentisierte und autorisierte Benutzer auf Daten zugreifen können und personenbezogene Daten vor unbefugtem Zugriff geschützt sind. Dies betrifft sowohl die Server, Datenbanken, Storage, Backup und Netzwerk Systeme in unseren	A.6.1.2 Aufgabentrennung A.6.2 Mobilgeräte und Telearbeit A.7.2.2 Informationssicherheitsbewusstsein, -ausbildung und -schulung	A.5.3 Aufgabentrennung A.5.12 Klassifizierung von Informationen A.5.15 Zugangssteuerung A.5.16 Identitätsmanagement

	DataCenter als auch die Client Systeme im Büro und unterwegs. Dies wird u.a. erreicht durch entsprechende Richtlinien, klar definierte Verantwortlichkeiten, durch eindeutige Identifikation, starke Authentisierung, Prozesse für Erhalt, Mutation und Entzug von Zugriffsberechtigungen, sicheren Fernzugriff, Protokollierung, initiale und wiederkehrende Security Awareness Schulungen sowie periodische Kontrollen und Audits.	A.8.2 Informationsklassifizierung A.9.1 Geschäftsanforderungen an die Zugangssteuerung A.9.2 Benutzerzugangsverwaltung A.9.3 Benutzerverantwortlichkeiten A.9.4 Zugangssteuerung für Systeme und Anwendungen A.12.4 Protokollierung und Überwachung	A.5.17 Authentisierungsinformationen A.5.18 Zugangsrechte A.5.34 Datenschutz und Schutz von personenbezogenen Daten(PbD) A.6.3 Informationssicherheitsbewusstsein, -ausbildung und -schulung A.6.7 Remote-Arbeit A.8.2 Privilegierte Zugangsrechte A.8.15 Protokollierung
b. nur berechtigte Personen Zugang zu den Räumlichkeiten und Anlagen haben, in denen Personendaten bearbeitet werden (**Zugangskontrolle**);	Zugangskontrolle umfasst organisatorische und technische Massnahmen zum Schutz von Datenverarbeitungssystemen vor unbefugten Nutzern. Dies betrifft sowohl die Server, Datenbanken, Storage, Backup und Netzwerk Systeme in unseren DataCenter als auch die Client Systeme im Büro und unterwegs. Dies wird u.a. erreicht durch entsprechende Richtlinien, klar definierte Verantwortlichkeiten, durch eindeutige Identifikation, Prozesse für Erhalt, Mutation und Entzug von Zutrittsberechtigungen, physische Zonen, sichere Schliess- und Zutrittssysteme, abgeschlossene Schränke für physische Personendaten, Begleitung von Besuchern, Protokollierung, initiale und wiederkehrende Security Awareness Schulungen sowie periodische Kontrollen und Audits.	A.6.1.2 Aufgabentrennung A.7.2.2 Informationssicherheitsbewusstsein, -ausbildung und -schulung A.8.2 Informationsklassifizierung A.9.1 Geschäftsanforderungen an die Zugangssteuerung A.11.1 Sicherheitsbereiche A.12.4 Protokollierung und Überwachung	A.5.3 Aufgabentrennung A.5.12 Klassifizierung von Informationen A.5.34 Datenschutz und Schutz von personenbezogenen Daten(PbD) A.6.3 Informationssicherheitsbewusstsein, -ausbildung und -schulung A.7.1 Physische Sicherheitsperimeter A.7.2 Physischer Zutritt A.7.3 Sichern von Büros, Räumen und Einrichtungen A.7.4 Physische Sicherheitsüberwachung A.8.15 Protokollierung

c. unbefugte Personen automatisierte Datenbearbeitungssysteme nicht mittels Einrichtungen zur Datenübertragung benutzen können (**Benutzerkontrolle**).	Benutzerkontrolle umfasst organisatorische und technische Massnahmen, die dafür sorgen, dass nur jene Personen Daten bearbeiten, die dazu berechtigt sind. Dies wird erreicht durch die Massnahmen der Zugriffskontrolle.	Siehe bei Zugriffskontrolle.	Siehe bei Zugriffskontrolle.
2 Um die **Verfügbarkeit** und **Integrität** zu gewährleisten, müssen der **Verantwortliche** und der **Auftragsbearbeiter** geeignete Massnahmen treffen, damit: a. unbefugte Personen Datenträger nicht lesen, kopieren, verändern, verschieben, löschen oder vernichten können (**Datenträgerkontrolle**);	Datenträgerkontrolle umfasst organisatorische und technische Massnahmen zum Schutz gespeicherter Daten (Data at Rest). Dies betrifft sowohl die Server, Datenbanken, Storage, Backup und Netzwerk Systeme in unseren DataCenter als auch die Client Systeme im Büro und unterwegs. Dies wird u.a. erreicht durch entsprechende Richtlinien, klar definierte Verantwortlichkeiten, Asset Management, Verschlüsselung von Datenträgern, Prozesse für Löschung oder Vernichtung nach entfallendem Zweck, Protokollierung, initiale und wiederkehrende Security Awareness Schulungen sowie periodische Kontrollen und Audits.	A.7.2.2 Informationssicherheitsbewusstsein, -ausbildung und -schulung A.8.1 Verantwortlichkeit für Werte A.8.2 Informationsklassifizierung A.8.3 Handhabung von Datenträgern A.11.2.6 Sicherheit von Geräten, Betriebsmitteln und Werten außerhalb der Räumlichkeiten A.11.2.7 sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln A.12.4 Protokollierung und Überwachung	A.5.9 Inventar der Informationen und anderen damit verbundenen Werte A.5.12 Klassifizierung von Informationen A.5.34 Datenschutz und Schutz von personenbezogenen Daten(PbD) A.6.3 Informationssicherheitsbewusstsein, -ausbildung und -schulung A.7.10 Speichermedien A.7.14 Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln A.8.10 Löschung von Informationen A.8.12 Verhinderung von Datenlecks A.8.15 Protokollierung
b. unbefugte Personen Personendaten im Speicher nicht speichern, lesen, ändern, löschen oder vernichten können (**Speicherkontrolle**);	Speicherkontrolle umfasst organisatorische und technische Massnahmen zum Schutz von Daten in flüchtigen Speichern (Data in Use) geschützt sind. Dies betrifft sowohl die Server, Datenbanken, Storage, Backup und	Siehe bei Datenintegrität.	Siehe bei Datenintegrität.

	Netzwerk Systeme in unseren DataCenter als auch die Client Systeme im Büro und unterwegs. Dies wird erreicht durch die Massnahmen der Datenintegrität.		
c. unbefugte Personen bei der Bekanntgabe von Personendaten oder beim Transport von Datenträgern Personendaten nicht lesen, kopieren, verändern, löschen oder vernichten können (**Transportkontrolle**);	Weitergabe- und Transportkontrolle umfasst organisatorische und technische Massnahmen zum Schutz von Daten beim logischem und physischem Transport (Data in Transit). Dies betrifft sowohl die Server, Datenbanken, Storage, Backup und Netzwerk Systeme in unseren DataCenter als auch die Client Systeme im Büro und unterwegs. Dies wird u.a. erreicht durch entsprechende Richtlinien, klar definierte Verantwortlichkeiten, authentisierte Sender und Empfänger, verschlüsselten Transport, Protokollierung, initiale und wiederkehrende Security Awareness Schulungen sowie periodische Kontrollen und Audits.	A.7.2.2 Informationssicherheitsbewusstsein, -ausbildung und -schulung A.8.1 Verantwortlichkeit für Werte A.8.2 Informationsklassifizierung A.8.3 Handhabung von Datenträgern A.10.1 Kryptographische Massnahmen A.11.2.6 Sicherheit von Geräten, Betriebsmitteln und Werten ausserhalb der Räumlichkeiten A.12.4 Protokollierung und Überwachung A.13.2 Informationsübertragung A.12.4 Protokollierung und Überwachung	A.5.9 Inventar der Informationen und anderen damit verbundenen Werte A.5.12 Klassifizierung von Informationen A.5.14 Informationsübermittlung A.5.34 Datenschutz und Schutz von personenbezogenen Daten(PbD) A.6.3 Informationssicherheitsbewusstsein, -ausbildung und -schulung A.7.14 Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln A.8.10 Löschung von Informationen A.8.12 Verhinderung von Datenlecks A.8.15 Protokollierung A.8.24 Verwendung von Kryptographie
d. die Verfügbarkeit der Personendaten und der Zugang zu ihnen bei einem physischen oder	Verfügbarkeit umfasst organisatorische und technische Massnahmen zum Schutz der Daten vor Verlust. Dies	A.8.2 Informationsklassifizierung	A.5.12 Klassifizierung von Informationen

technischen Zwischenfall rasch wiederhergestellt werden können **(Wiederherstellung);**	betrifft sowohl die Server, Datenbanken, Storage, Backup und Netzwerk Systeme in unseren DataCenter als auch die Client Systeme im Büro und unterwegs. Dies wird u.a. erreicht durch entsprechende Richtlinien, klar definierte Verantwortlichkeiten, unterbrechungsfreie Stromversorgung, redundante Systeme, regelmässige Datensicherung, periodische Wiederherstellungsstests, Notfallpläne und Audits.	A.12.3 Datensicherung A.17.1 Aufrechterhalten der Informationssicherheit A.17.2 Redundanzen A.12.4 Protokollierung und Überwachung	A.5.30 IKT-Bereitschaft für Business- Continuity A.8.13 Sicherung von Informationen A.8.14 Redundanz von informationsverarbeitenden Einrichtungen A.8.15 Protokollierung
e. alle Funktionen des automatisierten Datenbearbeitungssystems zur Verfügung stehen (Verfügbarkeit), Fehlfunktionen gemeldet werden (Zuverlässigkeit) und gespeicherte Personendaten nicht durch Fehlfunktionen des Systems beschädigt werden können (**Datenintegrität**);	Integrität umfasst organisatorische und technische Massnahmen zur Gewährleistung der Richtigkeit und Vollständigkeit der Daten. Dies betrifft sowohl die Server, Datenbanken, Storage, Backup und Netzwerk Systeme in unseren DataCenter als auch die Client Systeme im Büro und unterwegs. Dies wird u.a. erreicht durch entsprechende Richtlinien, klar definierte Verantwortlichkeiten, Berücksichtigung von Sicherheitsanforderungen in Entwicklung und Betrieb, Segmentierung von Netzwerken und Datenspeichern, System Hardening, Schwachstellen Management, Malware Protection, Monitoring, Protokollierung, initiale und wiederkehrende Security Awareness Schulungen sowie periodische Kontrollen und Audits.	A.7.2.2 Informationssicherheitsbewusstsein, -ausbildung und -schulung A.8.2 Informationsklassifizierung A.12.1 Betriebsabläufe und -verantwortlichkeiten A.12.2 Schutz vor Schadsoftware A.12.4 Protokollierung und Überwachung A.14.1 Sicherheitsanforderungen an Informationssysteme A.14.2 Sicherheit in Entwicklungs- und Unterstützungsprozessen A.18.1.3 Schutz von Aufzeichnungen	A.5.12 Klassifizierung von Informationen A.5.33 Schutz von Aufzeichnungen A.5.34 Datenschutz und Schutz von personenbezogenen Daten(PbD) A.5.37 Dokumentierte Betriebsabläufe A.6.3 Informationssicherheitsbewusstsein, -ausbildung und -schulung A.8.9 Konfigurationsmanagement A.8.15 Protokollierung A.8.32 Änderungssteuerung
f. Betriebssysteme und Anwendungssoftware stets auf dem neusten Sicherheitsstand gehalten und bekannte kritische Lücken geschlossen werden (**Systemsicherheit**).	Systemsicherheit umfasst alle betrieblichen Sicherheitsaspekte. Dies betrifft sowohl die Server, Datenbanken, Storage, Backup und Netzwerk Systeme in unseren DataCenter als auch die Client Systeme im Büro und unterwegs.	Siehe bei Zugriffs- und Zugangkontrolle, Datenträger-, Speicher- und Transportkontrolle sowie	Siehe bei Zugriffs- und Zugangkontrolle, Datenträger-, Speicher- und Transportkontrolle sowie bei

	Dies wird erreicht durch die Massnahmen für Zugriffs- und Zugangkontrolle, die Massnahmen für Datenträger-, Speicher- und Transportkontrolle sowie die Massnahmen für Verfügbarkeit und Integrität.	bei Verfügbarkeit und Integrität.	Verfügbarkeit und Integrität.
3 Um die **Nachvollziehbarkeit** zu gewährleisten, müssen der **Verantwortliche** und der **Auftragsbearbeiter** geeignete Massnahmen treffen, damit: a. überprüft werden kann, welche Personendaten zu welcher Zeit und von welcher Person im automatisierten Datenbearbeitungssystem eingegeben oder verändert werden (**Eingabekontrolle**);	Eingabekontrolle umfasst organisatorische und technische Massnahmen zur Gewährleistung der Nachvollziehbareit der Datenbearbeitungen, d.h. von Erfassung, Speicherung, Veränderung, Übertragung, Sicherung, Archivierung und Löschung. Dies wird u.a. erreicht durch entsprechende Richtlinien, klar definierte Verantwortlichkeiten, ein Verzeichnis der Datenbearbeitungen, Monitoring, Protokollierung, initiale und wiederkehrende Security Awareness Schulungen sowie periodische Kontrollen und Audits.	A.7.2.2 Informationssicherheitsbewusstsein, -ausbildung und -schulung A.8.1 Verantwortlichkeit für Werte A.8.2 Informationsklassifizierung A.12.4 Protokollierung und Überwachung A.18.1.3 Schutz von Aufzeichnungen	A.5.9 Inventar der Informationen und anderen damit verbundenen Werte A.5.12 Klassifizierung von Informationen A.5.33 Schutz von Aufzeichnungen A.5.34 Datenschutz und Schutz von personenbezogenen Daten(PbD) A.6.3 Informationssicherheitsbewusstsein, -ausbildung und -schulung A.8.15 Protokollierung A.8.16 Überwachung von Aktivitäten
b. überprüft werden kann, wem Personendaten mit Hilfe von Einrichtungen zur Datenübertragung bekanntgegeben werden (**Bekanntgabekontrolle**);	Bekanngabekontrolle umfasst organisatorische und technische Massnahmen zur Gewährleistung der Nachvollziehbareit der Datenbearbeitungen, d.h. von Erfassung, Speicherung, Veränderung, Übertragung, Sicherung, Archivierung und Löschung. Dies wird erreicht durch die Massnahmen für Zugriffskontrolle, Transportkontrolle und Eingabekontrolle.	Siehe bei Zugriffskontrolle, Transportkontrolle und Eingabekontrolle.	Siehe bei Zugriffskontrolle, Transportkontrolle und Eingabekontrolle.
c. Verletzungen der Datensicherheit rasch erkannt (**Erkennung**) und Massnahmen zur Minderung oder Beseitigung der Folgen ergriffen werden können (**Beseitigung**).	Erkennung und Beseitigung umfasst organisatorische und technische Massnahmen, damit potentielle und tatsächliche Verletzungen der Datensicherheit erkannt, analysiert, bewertet, behandelt und kommuniziert werden.	A.6.1.3 Kontakt mit Behörden	A.5.24 Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen

	Dies wird u.a. erreicht durch entsprechende Richtlinien, klar definierte Verantwortlichkeiten, Verpflichtung zur Meldung von Sicherheitsrisiken und Sicherheitsvorfällen, Kontakt mit Behörden, initiale und wiederkehrende Security Awareness Schulungen sowie periodische Kontrollen und Audits.	A.7.2.2 Informationssicherheitsbewusstsein, -ausbildung und -schulung A.7.2.3 Massregelungsprozess A.16.1 Handhabung von Informationssicherheitsvorfällen und Verbesserungen	A.5.25 Beurteilung und Entscheidung über Informationssicherheitsereignisse A.5.26 Reaktion auf Informationssicherheitsvorfälle A.5.27 Erkenntnisse aus Informations- sicherheitsvorfällen A.5.28 Sammeln von Beweismaterial A.5.33 Schutz von Aufzeichnungen A.5.34 Datenschutz und Schutz von personenbezogenen Daten(PbD) A.6.3 Informationssicherheitsbewusstsein, -ausbildung und -schulung A.6.4 Massregelungsprozess

[1] bis spätestens Oktober 2025
[2] ab spätestens Oktober 2025