

Datenschutz-Richtlinie

der

Medset Medizintechnik GmbH

I. Allgemeines

1. Einleitung

- 1.1 Die in der Medset vorhandenen Daten sind für Medset und die reibungslosen Abläufe im Unternehmen von großem Wert. Diese Daten sind daher gegen unbefugte Zugriffe und andere Gefährdungen zu schützen.
- 1.2 Gleichzeitig erwarten die Kunden, Partner und Mitarbeiter der Medset, dass die der Medset anvertrauten Daten besonders geschützt werden und ein sorgsamer Umgang mit ihnen erfolgt.
- 1.3 Medset bekennt sich auch im Rahmen seines gesellschaftlichen Engagements zu seiner Verantwortung für den sorgsamen Umgang mit personenbezogenen Daten.

2. Ziel der Datenschutz-Richtlinie

- 2.1 Mit dieser Datenschutz-Richtlinie sollen einheitliche Standards für den Datenschutz in der Medset geschaffen und nach außen kommuniziert werden.
- 2.2 Durch die Einhaltung der in dieser Datenschutz-Richtlinie definierten Standards kommt Medset seinen datenschutzrechtlichen Verpflichtungen nach und sorgt für eine ausreichende Berücksichtigung der Interessen sowie Rechte der betroffenen Personen.
- 2.3 Die Beachtung dieser Datenschutz-Richtlinie ist Voraussetzung für den sicheren Austausch von personenbezogenen Daten innerhalb der Medset.

3. Anwendungsbereich der Datenschutz-Richtlinie

- 3.1 Diese Datenschutz-Richtlinie gilt für jegliche Verarbeitung von personenbezogenen Daten, wobei die erstmalige Erfassung von Daten, deren Speicherung und Verwendung sowie die Weitergabe innerhalb der Medset und die Übermittlung an Dritte erfasst werden.
- 3.2 Sofern sich aus den gesetzlichen Bestimmungen geringere Anforderungen ergeben, gelten die Regelungen dieser Datenschutz-Richtlinie.

II. Grundsätze der Datenverarbeitung

4. Zulässigkeit der Datenverarbeitung

- 4.1 Bei jedem Vorgang der Datenverarbeitung ist zu prüfen, ob die beabsichtigte Verarbeitung von Daten zulässig ist. Bestehen Zweifel an der Zulässigkeit, soll der Datenschutzbeauftragte kontaktiert werden.
- 4.2 Die Zulässigkeit der Datenverarbeitung kann sich aus verschiedenen Gesichtspunkten ergeben. Zunächst kann sich die Zulässigkeit daraus ergeben, dass der Betroffene in die Datenverarbeitung

eingewilligt hat. Auch ohne Einwilligung des Betroffenen kann die Datenverarbeitung zulässig sein, wenn eine gesetzliche Ermächtigungsgrundlage vorliegt. Fehlt es an einer Einwilligung und einer gesetzlichen Ermächtigungsgrundlage, dann ist die Datenverarbeitung unzulässig.

5. Gesetzliche Ermächtigungsgrundlagen

- 5.1 Die Verarbeitung personenbezogener Daten kann erforderlich sein für die Begründung oder Erfüllung eines Vertrags mit der betroffenen Person. Im Rahmen unserer Datenverarbeitung von Gesundheitsdaten kommen insbesondere § 203 StGB Abs. 3 StGB i.V.m. Art. 9 Abs. 2 lit. i) DSGVO i.V.m. § 22 Abs. 1 Ziffer 1 b) BDSG (neu) bzw. Art. 28 i.V.m. Art. 4 Nr. 7, 8 und 15 DSGVO i.V.m. § 22 BDSG (neu) im Bereich der Auftragsverarbeitung als Rechtsgrundlage für die Datenübermittlung in Betracht.
- 5.2 Eine Notwendigkeit und Ermächtigung zur Datenverarbeitung kann sich aufgrund einer rechtlichen Verpflichtung der Medset ergeben. Als Ermächtigungsgrundlage kommt insbesondere ein Auskunftsersuchen von Ermittlungsbehörden in Betracht.
- 5.3 Zulässig ist die Verarbeitung personenbezogener Daten auch, wenn sie zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche vor Gericht erforderlich ist. Gleiches gilt für die Wahrung lebenswichtiger Interessen.
- 5.4 Denkbar ist eine Datenverarbeitung schließlich in den Fällen, bei denen die Verarbeitung für die Erfüllung eines Vertrages erforderlich ist oder berechtigte Interessen der Medset bestehen und gleichzeitig kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Datenverarbeitung überwiegt. Das Ergebnis einer solchen Interessenabwägung soll dabei schriftlich protokolliert werden.

6. Einwilligung und Protokollierung

- 6.1 Eine Einwilligung der betroffenen Person ist als Grundlage für die Datenverarbeitung ausreichend, wenn die betroffene Person zuvor ausreichend informiert wurde und ihre Einwilligung für die beabsichtigte Datenverarbeitung anschließend eindeutig und auf freiwilliger Basis erteilt hat.
- 6.2 Von einer ausreichenden Information ist auszugehen, wenn die wesentlichen Abläufe der Datenverarbeitung verständlich erläutert werden und insbesondere erklärt wird, zu welchem Zweck die Daten verarbeitet werden. Die betroffene Person soll darauf hingewiesen werden, dass ihre Einwilligung widerruflich ist. Außerdem ist darauf zu achten, dass Einwilligungserklärungen gegenüber anderen Erklärungen optisch hervorgehoben und abgegrenzt werden. Eine Kopplung der Einwilligung mit anderen Erklärungen soll vermieden werden.

7. Zweckbindung

- 7.1 Personenbezogene Daten dürfen nur für den Zweck verarbeitet werden, für den sie ursprünglich erhoben wurden. Bei Einholung einer Einwilligung von der betroffenen Person ist auf den konkreten Zweck hinzuweisen. Es muss sich stets um einen rechtmäßigen Zweck der Datenverarbeitung handeln.
- 7.2 Wenn später eine Datenverarbeitung zu einem anderen Zweck erfolgen soll, dann muss auch hierfür eine Einwilligung eingeholt werden oder eine gesetzliche Ermächtigungsgrundlage vorliegen, sofern der neue Zweck der Datenverarbeitung nicht bereits mit dem ursprünglichen Zweck vereinbar ist.

8. Verhältnismäßigkeit

- 8.1 Bei der Verarbeitung personenbezogener Daten ist der Grundsatz der Verhältnismäßigkeit zu

beachten. Der Grundsatz der Verhältnismäßigkeit ist beachtet, wenn die Datenverarbeitung dazu geeignet ist, einen legitimen Zweck zu erreichen. Weiter darf kein milderer, gleichermaßen geeignetes Mittel zur Erreichung des vorgesehenen Zwecks zur Verfügung stehen. Schließlich ist zu prüfen, ob der Datenverarbeitung keine überwiegenden schutzwürdigen Interessen der betroffenen Person entgegenstehen.

- 8.2 Als milderer Mittel kann bspw. die Verarbeitung von aggregierten Daten oder sonstigen Daten ohne Personenbezug in Betracht kommen.

9. Datenminimierung

- 9.1 Die Datenverarbeitung in der Medset ist so zu organisieren, dass so wenig personenbezogene Daten wie möglich verarbeitet werden. Wenn personenbezogene Daten nicht mehr benötigt werden, sollen diese gelöscht werden.
- 9.2 Bereits bei der Datenerhebung ist darauf zu achten, dass als Voreinstellung nur die zwingend benötigten Daten verlangt und alle weiteren Daten auf freiwilliger Basis erhoben werden. Voreinstellungen und Vorgaben für betroffene Personen sollen möglichst datenschutzfreundlich gestaltet sein.
- 9.3 Für die in der Medset gespeicherten Daten ist festzulegen, für welchen Zeitraum eine Aufbewahrung bzw. Speicherung zu erfolgen hat. Gesetzliche Aufbewahrungspflichten sind hierbei zu beachten. Nach Ablauf der Aufbewahrungsfrist bzw. Speicherdauer ist für eine Löschung der Daten zu sorgen, idealerweise durch ein automatisiertes Verfahren.

10. Datensicherheit

- 10.1 Für Medset ist von großer Bedeutung, dass die Sicherheit der Daten jederzeit gewährleistet ist. Vor diesem Hintergrund sind die Daten u.a. ausreichend gegen Verlust, gegen unbefugten Zugriff und vor anderen Gefahren zu schützen.
- 10.2 Es ist daher dafür zu sorgen, dass angemessene Maßnahmen getroffen werden, um personenbezogene Daten zu schützen. Der Schutz hat durch technische und organisatorische Maßnahmen zu erfolgen.
- 10.3 Für die einzelnen Vorgänge der Datenverarbeitung sind die konkreten Schutzmaßnahmen zu dokumentieren und auf ihre Angemessenheit zu überprüfen.

III. Spezielle Formen der Datenverarbeitung im Gesundheitswesen

11. Verarbeitung besonderer Arten von Daten

- 11.1 Bei der Verarbeitung von personenbezogenen Daten ist zu berücksichtigen, dass sensible Daten und Daten über besonders schützenswerte betroffene Personen nur bei Vorliegen von zusätzlichen Voraussetzungen und/oder bei Einhaltung besonderer Schutzmaßnahmen verarbeitet werden dürfen.
- 11.2 Ein besonderer Schutz besteht für Gesundheitsdaten. Für die Verarbeitung der vorgenannten Kategorien von Daten bedarf es einer gesonderten Rechtfertigung, außerdem sind geeignete Sicherheitsvorkehrungen zu implementieren und zu dokumentieren.
- 11.3 Medset beachtet die gesetzlichen Regelungen zur Berufsverschwiegenheit und erklärt sich bereit, eine Verschwiegenheits-Erklärung unter bestimmten Voraussetzungen abzugeben.

12. Auftragsverarbeitung

- 12.1 Wenn Dienstleister der Medset in dessen Auftrag personenbezogene Daten verarbeiten oder Medset als Dienstleister für Dritte Daten verarbeitet, werden die Vorschriften der Art. 4 Nr. 7, 8 und 15, Art. 9 Abs. 2 lit. i) DSGVO und Art. 28 DSGVO i.V.m. § 22 Abs. 1 Ziffer 1 b) BDSG (neu) beachtet werden.
- 12.2 Der Dienstleister wird im Auftrag und auch unter der Verantwortung der Medset tätig. Spätestens mit Beginn der Tätigkeit für Medset ist dafür Sorge zu tragen, dass mit dem Dienstleister eine gesonderte Vereinbarung zur Auftragsverarbeitung vereinbart wird und danach eine regelmäßige Kontrolle der Einhaltung der Pflichten aus der Vereinbarung zur Auftragsverarbeitung erfolgt. Dies gilt ebenfalls, wenn Medset als Dienstleister im Auftrag Dritter Daten verarbeitet.

IV. Innerbetriebliche Prozesse

13. Anforderungen an Mitarbeiter

- 13.1 Alle Mitarbeiter der Medset sind besonders auf das Datengeheimnis zu verpflichten. Sie sind darüber zu belehren, dass es untersagt ist, personenbezogene Daten für private Zwecke zu nutzen, an Unbefugte zu übermitteln oder sie Unbefugten zugänglich zu machen. Die Verpflichtung auf das Datengeheimnis soll mit Beginn der Tätigkeit für Medset erfolgen. Die Mitarbeiter sind darüber zu belehren, dass die Pflicht zur Wahrung der Vertraulichkeit über das Ende der Tätigkeit für Medset fortgilt.
- 13.2 Auch innerhalb der Medset ist darauf zu achten, dass nur die Mitarbeiter Zugriff auf personenbezogene Daten erhalten, die sie zur Erledigung ihrer Aufgaben für Medset benötigen.
- 13.3 Alle Mitarbeiter sollen zu Beginn ihrer Tätigkeit und nachfolgend regelmäßig in Datenschutzthemen geschult werden.

14. Dokumentationspflichten

- 14.1 Medset führt ein Verzeichnis über die Verfahren der Medset zur Verarbeitung personenbezogener Daten (Verzeichnis der Verarbeitungstätigkeiten), das von dem Datenschutzbeauftragten verwaltet wird.
- 14.2 Um das Verzeichnis der Verarbeitungstätigkeiten vollständig und aktuell zu halten, haben die Mitarbeiter entsprechend den Vorgaben des Datenschutzbeauftragten alle Verfahren unter Nutzung entsprechender Vordrucke zu melden.

V. Rechte der betroffenen Personen

15. Recht auf Auskunft und Datenübertragbarkeit

- 15.1 Auf Anfrage ist einer betroffenen Person mitzuteilen, ob von Medset personenbezogene Daten zu ihrer Person verarbeitet werden. Sofern dies der Fall ist, hat die betroffene Person einen Anspruch auf Auskunft über die entsprechenden personenbezogenen Daten. Die betroffene Person soll dabei die Art der Daten, zu denen sie eine Auskunft wünscht, näher bezeichnen.
- 15.2 Die Auskunftserteilung soll in einer für die betroffene Person verständlichen Form und Sprache erfolgen. Bei der Auskunftserteilung sind die vorhandenen personenbezogenen Daten und der Zweck der Speicherung mitzuteilen. Weiter soll, soweit verfügbar, die Herkunft der Daten erläutert werden. Verpflichtend sind außerdem Angaben zu etwaigen Empfängern der Daten, die Dauer der

Speicherung, einer etwaigen automatisierten Entscheidungsfindung sowie Hinweise auf die Betroffenenrechte und das Beschwerderecht bei der Aufsichtsbehörde.

- 15.3 Neben dem Auskunftsrecht steht der betroffenen Person grundsätzlich auch der Anspruch zu, die zu ihrer Person gespeicherten Daten in strukturierter Form zu erhalten, damit diese von einem anderen Verantwortlichen übernommen werden können. Dieses Recht auf Datenübertragbarkeit bezieht sich aber nur auf solche Daten, die auf Basis einer Einwilligung, zur Erfüllung eines Vertrages oder im Rahmen einer automatisierten Verarbeitung verarbeitet wurden.
- 15.4 Bei der Auskunftserteilung und Erfüllung des Anspruchs auf Datenübertragbarkeit ist sicherzustellen, dass die Identität der betroffenen Person verifiziert wird. Weiter ist zu beachten, dass im Rahmen der Auskunftserteilung keine personenbezogenen Daten Dritter offenbart werden.
- 15.5 Über alle Anfragen auf Auskunftserteilung oder Ansprüche auf Datenübertragbarkeit ist der Datenschutzbeauftragte zu informieren, damit dieser die weiteren Aktivitäten koordinieren oder übernehmen kann. Soweit der Datenschutzbeauftragte nicht ausdrücklich die Bearbeitung übernimmt, bleibt die jeweilige Fachabteilung für die Beantwortung der Anfrage zuständig.
- 15.6 Wenn eine Anfrage nicht umgehend beantwortet bzw. ein Anspruch nicht umgehend erfüllt werden kann, ist der betroffenen Person zumindest eine Zwischeninformation zu übermitteln, in der die voraussichtliche Bearbeitungszeit mitgeteilt werden soll.

16. Löschung und Einschränkung der Verarbeitung

- 16.1 Bei berechtigtem Anspruch einer betroffenen Person sind die zu ihrer Person gespeicherten personenbezogenen Daten zu löschen. Ein Anspruch ist insbesondere berechtigt, wenn keine Grundlage für die Datenverarbeitung besteht oder die Grundlage zwischenzeitlich entfallen ist. Sofern keine Grundlage (mehr) für die Speicherung von personenbezogenen Daten besteht, sind diese unabhängig von einem Anspruch der betroffenen Person zu löschen.
- 16.2 Soweit eine Löschung nicht in Betracht kommt, ist zu prüfen, inwieweit zumindest eine Einschränkung der Verarbeitung der personenbezogenen Daten erfolgen kann. Eine Einschränkung der Verarbeitung soll insbesondere bis zur Klärung der Zulässigkeit der weiteren Datenverarbeitung erfolgen. Wenn die betroffene Person die weitere Nutzung ihrer Daten nicht mehr wünscht, ist eine Einschränkung der Verarbeitung in Erwägung zu ziehen, damit die Daten der betroffenen Person im Falle einer neuen Datenerhebung nicht (wieder) genutzt werden.

17. Recht auf Berichtigung

- 17.1 Unvollständige oder unrichtige personenbezogene Daten sind auf Verlangen der betroffenen Person zu korrigieren. Die Korrektur ist dabei auch im Interesse der Medset, da der gesamte Datenbestand möglichst richtig und von hoher Qualität sein soll.
- 17.2 Soweit ein Mitarbeiter Kenntnis davon hat, dass bei Medset gespeicherte Daten unvollständig und unrichtig sind, soll der Mitarbeiter die jeweilige Fachabteilung hierüber informieren, damit eine Korrektur veranlasst werden kann.

18. Recht auf Widerruf, Widerspruch und Beschwerde

- 18.1 Eine von einer betroffenen Person erteilte Einwilligung in die Verarbeitung ihrer Daten ist jederzeit widerruflich. Die betroffene Person ist auf die Möglichkeit des Widerrufs hinzuweisen. Der Widerruf gilt mit Wirkung für die Zukunft.

- 18.2 Soweit die Verarbeitung von Daten auf Basis einer gesetzlichen Ermächtigungsgrundlage erfolgt, bedarf es keiner Einwilligung der betroffenen Person. Widerspricht die betroffene Person der Datenverarbeitung, ist zu prüfen, inwieweit auf die Datenverarbeitung zukünftig verzichtet werden kann. Ist dies nicht möglich, ist der betroffenen Person dies entsprechend zu erläutern.
- 18.3 Die betroffene Person hat das Recht, sich über den Umgang mit ihren personenbezogenen Daten bei Medset zu beschweren. Die Beschwerde ist unverzüglich an den Datenschutzbeauftragten weiterzuleiten, sofern sie nicht an ihn direkt gerichtet war. Der Datenschutzbeauftragte wird die Beschwerde beantworten und ggf. angemessene Maßnahmen zur Verbesserung des Datenschutzniveaus vorschlagen.

VI. Zuständigkeit

19. Verantwortung

- 19.1 In erster Linie sind diejenigen Mitarbeiter für die Einhaltung der Vorgaben dieser Datenschutz-Richtlinie verantwortlich, die jeweils mit der Datenverarbeitung betraut sind.
- 19.2 Alle Mitarbeiter der Medset haben auf die Einhaltung dieser Datenschutz-Richtlinie zu achten und auf diese Weise dazu beizutragen, dass in der gesamten Medset einheitlich hohe Datenschutzstandards etabliert werden.
- 19.3 Die Führungskräfte der Medset haben darauf zu achten, dass die Mitarbeiter über die Datenschutz-Richtlinie informiert werden. Zu der Information gehört auch der Hinweis, dass Verstöße gegen die Vorgaben dieser Datenschutz-Richtlinie straf-, haftungs- oder arbeitsrechtliche Konsequenzen nach sich ziehen können.
- 19.4 Medset bleibt gegenüber der betroffenen Person der Verantwortliche im datenschutzrechtlichen Sinne. Der einzelne Mitarbeiter handelt daher für Medset und hat dessen Vorgaben zu beachten.

20. Datenschutzbeauftragter als Ansprechpartner

- 20.1 Fragen zu dieser Datenschutz-Richtlinie oder dem richtigen Umgang mit personenbezogenen Daten können an den Datenschutzbeauftragten gerichtet werden.
- 20.2 Der Datenschutzbeauftragte koordiniert die datenschutzrechtlichen Aktivitäten der Medset. Er ist u.a. Ansprechpartner für die betroffenen Personen, für die mit der Datenverarbeitung betrauten Mitarbeiter und für die Geschäftsführung.
- 20.3 Der Datenschutzbeauftragte ist auch befugt, die Einhaltung dieser Datenschutz-Richtlinie zu prüfen und die Beachtung der gesetzlichen Bestimmungen des Datenschutzrechts zu überwachen. Die entsprechende Überwachungsbefugnis entbindet aber nicht den einzelnen Mitarbeiter von seiner Verantwortung.
- 20.4 Alle Mitarbeiter haben den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben und Aktivitäten zu unterstützen. Der Datenschutzbeauftragte kann sich in Erfüllung seiner Aufgaben jederzeit an die Geschäftsführung wenden und seine Anliegen vortragen.

21. Meldung von Verstößen und Zusammenarbeit mit Aufsichtsbehörden

- 21.1 Die Mitarbeiter haben dem Datenschutzbeauftragten unverzüglich Bericht zu erstatten, wenn sie Kenntnis von einem Verstoß gegen diese Datenschutz-Richtlinie oder gesetzliche Bestimmungen haben, die sich auf den Schutz personenbezogener Daten beziehen.
- 21.2 Eine Information hat bereits dann zu erfolgen, wenn erste Anhaltspunkte oder Verdachtsmomente

für einen Datenschutzverstoß vorliegen. Auf diese Weise soll der Datenschutzbeauftragte frühzeitig in die Aufklärung der Angelegenheit eingebunden werden. Weitere Details im Hinblick auf das Verhalten bei möglichen Datenschutzverstößen sind in einem gesonderten Konzept für Datenschutzverstöße definiert.

- 21.3 Auf Basis der erhaltenen Informationen prüft der Datenschutzbeauftragte, inwieweit eine Informationspflicht gegenüber den Aufsichtsbehörden und den betroffenen Personen besteht.
- 21.4 Medset arbeitet mit den zuständigen Aufsichtsbehörden kooperativ und vertrauensvoll zusammen. Im Falle einer gesetzlichen Auskunftspflichtung wird Medset die geforderten Auskünfte unverzüglich erteilen. Maßnahmen und Feststellungen der Aufsichtsbehörden werden von Medset uneingeschränkt akzeptiert, soweit sie rechtmäßig sind. Die Kommunikation mit den Aufsichtsbehörden soll über den Datenschutzbeauftragten erfolgen.

22. Änderungen dieser Datenschutz-Richtlinie

- 22.1 Medset behält sich das Recht vor, diese Datenschutz-Richtlinie bei Bedarf zu ändern. Eine Änderung kann insbesondere erforderlich werden, um gesetzlichen Vorgaben, bindenden Verordnungen, Forderungen der Aufsichtsbehörden oder interne Verfahren der Medset zu entsprechen.
- 22.2 In regelmäßigen Abständen soll auch geprüft werden, inwieweit technologische Veränderungen eine Anpassung dieser Datenschutz-Richtlinie erforderlich machen.

Hamburg, den 25. Mai 2018



Klaus Kophstahl