Gesund, aktiv, datengeschützt

HINTERGRUND. Wer Wearables und Gesundheits-Apps im BGM einsetzt, muss den Schutz der Mitarbeiterdaten sicherstellen. Wir zeigen, was dabei zu beachten ist.

Von **Fabian Krapf, Uwe Klaus Schneider** und **Utz Niklas Walter**

Mit sehr hoher Geschwindigkeit und in einer nahezu unüberschaubaren Vielfalt verbreiten sich digitale Technologien wie Gesundheits-Apps, Wearables und Gesundheits-Portale auf dem Gesundheitsmarkt. Auch in vielen Unternehmen und Behörden werden diese virtuellen Gesundheitshelfer bereits erfolgreich im Kontext Betrieblicher Gesundheitsförderung (BGF) eingesetzt. Zwangsläufig sehen sich immer mehr Personal- und Gesundheitsverantwortliche daher mit der Frage konfrontiert, wie es um den Schutz der mitunter hochsensiblen Daten bestellt ist. Welche Vorkehrungen sind zu treffen, um Missbrauch zu verhindern? Und wie sollten Beschäftigte informiert und eingebunden werden, um bestehende Bedenken zu mindern?

© YOUTUBE

VIDEO

Mit dem Datenschutz beim Einsatz von Wearables beschäftigte sich auch der Safer Internet Day. In unserer App sehen Sie die wichtigsten Ergebnisse im Video.

Vor dem Hintergrund der teils berechtigten Bedenken ist die intensive Auseinandersetzung mit Fragen der Datensicherheit und des Datenschutzes unerlässlich, wenn Maßnahmen der digitalen BGF erfolgreich in Unternehmen oder Behörden implementiert werden sollen.

Zweck und Umfang des Schutzes von Gesundheitsdaten

Zweck des Datenschutzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. So formuliert es § 1 Abs. 1 des Bundesdatenschutzgesetzes (BDSG), welches den Datenschutz durch private Stellen, Unternehmen und Organisationen sowie für Bundesbehörden – auch als Arbeitgeber – näher ausgestaltet. Bei dem im Hintergrund stehenden Persönlichkeitsrecht handelt es sich um ein Grundrecht, das dem Schutz einer Person vor Eingriffen in ihren privaten Lebens- und Freiheitsbereich dient. Geschützt wird hierdurch die freie Entfaltung der Persönlichkeit und somit auch die individuelle Abwägung, ob ein mehr oder weniger gesundheitsförderlicher Lebensstil gepflegt werden soll. Um insoweit tatsächlich eine freie Entscheidung zu ermöglichen, sind grundsätzlich auch Benachteiligungen aufgrund von ungesundem Verhalten oder gesundheitlichen Beeinträchtigungen zu vermeiden. Die Angst vor solchen Benachteiligungen sowie das Risiko dahingehend soll die freie Entfaltung der Persönlichkeit nicht bereits im Vorfeld beeinträchtigen.

Das Persönlichkeitsrecht sieht überdies vor, dass jeder Mensch selbst entscheiden können sollte, wie er sich Dritten oder der Öffentlichkeit gegenüber darstellen will. Dies schließt neben dem Recht am gesprochenen beziehungsweise geschriebenen Wort, dem Recht am eigenen Bild und einigen weiteren auch das Recht auf informationelle Selbstbestimmung mit ein. Dieses Recht besagt, dass der Einzelne bestimmen darf, welche ihn betreffenden Daten weitergeleitet oder verwendet werden dürfen. Dies führt zu einer Erweiterung des Schutzes im Vorfeld von eventuellen manifesten Benachteiligungen und Beeinträchtigungen des Persönlichkeitsrechts, denn diese setzen üblicherweise an Informationen über den Einzelnen an.

Geschützt werden um des Persönlichkeitsrechts willen nur personenbezogene Daten. Dabei handelt es sich um Einzelangaben über persönliche oder sachliche Verhältnisse (zum Beispiel Arbeitgeber) einer bestimmten oder bestimmbaren Person (§ 3 Abs. 1 BDSG). Bestimmt bedeutet in diesem Zusammenhang, dass die Person namentlich bekannt ist. Bestimmbar meint, dass sie beispielsweise anhand der Personalnummer oder der IP-Adresse identifiziert werden könnte. Anonym erhobene Informationen zählen folglich nicht hierzu.

Gesundheitsdaten sind eine besondere Form von personenbezogenen Daten (§ 3 Abs. 9 BDSG) und umfassen nicht nur negative Abweichungen vom Normalzustand (beispielsweise Krankheit, Beschwerden), sondern auch positive Aussagen zur gesundheitlichen Verfassung (beispielsweise Fitness, Leistungsfähigkeit). Für sie

Wearables in der Betrieblichen Gesundheitsförderung können sinnvoll sein – aber der Datenschutz muss stimmen.

gilt ein besonders strenger Datenschutz (vgl. § 28 Absatz 6 bis 9 BDSG). So ist der Datenumgang für Zwecke der Gesundheitsversorgung und -vorsorge allein aufgrund des Gesetzes nur Personen erlaubt, die der ärztlichen Schweigepflicht oder einer entsprechenden Geheimhaltungspflicht unterliegen. Neben diesen besonderen Auflagen für Gesundheitsdaten gilt es im Hinblick auf den Schutz aller personenbezogenen Daten verschiedene Grundprinzipien zu berücksichtigen.

Drei Grundprinzipien zum Umgang mit Daten im Gesundheitsmanagement

Möchte ein Unternehmen Maßnahmen der digitalen Gesundheitsförderung im Betrieb umsetzen und hierzu von der Belegschaft personenbezogene Daten erheben, müssen hierfür drei Grundprinzipien berücksichtigt werden: Der Datenumgang muss sicher und transparent erfolgen und bedarf zudem einer Rechtsgrundlage.

Sicherheit des Datenumgangs: Zunächst einmal muss dafür Sorge getragen werden, dass technische und organisatorische Maßnahmen ein angemessenes, das bedeutet bei Gesundheitsdaten ein sehr hohes Maß an Sicherheit gewähren. Dazu gehört etwa, dass die sensiblen Daten lediglich in verschlüsselter Form transportiert und eventuell auch nur in dieser Form gespeichert werden. Zudem sollte für den administrativen Vollzugriff auf die Gesundheitsdaten aller Betroffenen, wenn dieser überhaupt möglich sein soll, das Vier-Augen-Prinzip angewandt werden, um auf diese Weise die Wahrscheinlichkeit von Fehlern oder Missbrauch zu reduzieren.

Transparenz im Datenumgang: Der Umgang mit den Daten sollte für die Betroffenen transparent gestaltet sein. Hierzu zählt beispielsweise, im Vorfeld der Datenerhebung zu erklären, welche Daten zu welchem Zweck auf welchem Wege erhoben werden und wie diese nachfolgend verarbeitet, gespeichert und wieder gelöscht werden. Reaktiv muss dem Betroffenen auf Wunsch Auskunft über die zu seiner Person gespeicherten Daten erteilt werden – mit der Möglichkeit einer Korrektur im Anschluss.

Rechtsgrundlage für den Datenumgang: Bezüglich des Umgangs mit personenbezogenen Daten besteht im deutschen und europäischen Datenschutzrecht ein sogenanntes Verbot mit Erlaubnisvorbehalt. Hierdurch wird ein Prinzip definiert, wonach jedwedes Erheben, Verarbeiten und/oder Nutzen von personenbezogenen Daten verboten ist, es sei denn, ein Gesetz oder die Einwilligung des Betroffenen rechtfertigen dies. Für die Umsetzung von Maßnahmen aus dem Bereich E-Health im Betrieb, bei der eine Vielzahl dieser Daten erhoben und verarbeitet wird, bedarf es daher (a) einer gesetzlichen Grundlage, (b) einer Betriebs- beziehungsweise Dienstvereinbarung oder (c) einer Einwilligung des Beschäftigten.

Eine gesetzliche Grundlage könnte sich aus § 32 Abs. 1 BDSG ergeben, wonach personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden dürfen, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder für dessen Durchführung oder Beendigung erforderlich ist. Maßnahmen der betrieblichen Gesundheitsförderung können im Rahmen des Beschäftigungsverhältnisses zwar sehr wohl sinnvoll sein, sie sind für die genannten Zwecke

in aller Regel aber nicht erforderlich. Eine ausreichende Rechtsgrundlage ergibt sich also nicht allein aus dem Gesetz.

Eine Betriebs- beziehungsweise Dienstvereinbarung zwischen Arbeitgeber und Betriebs- oder Personalrat kann auch verbindliche Normen für alle Arbeitnehmer eines Betriebs formulieren. In einer solchen Vereinbarung können Details hinsichtlich des Datenumgangs innerhalb des Unternehmens für die Arbeitnehmer spezifiziert werden. Im höchstpersönlichen Bereich der Erfassung von Gesundheitsdaten für Zwecke der BGF sollte allerdings jeder betroffene Beschäftigte selbst einwilligen. Mit einer entsprechenden Einwilligung drückt der Beschäftigte im Vorfeld sein Einverständnis mit der Datenerhebung, -nutzung und -verarbeitung aus. Da dieser Aspekt für die praktische Durchführung von gesundheitsförderlichen Maßnahmen in Unternehmen und Behörden besondere Relevanz besitzt, wird er im nachfolgenden Kapitel detailliert ausgeführt.

Kernstück der Information ist die Einwilligung durch die Mitarbeiter

Kernstück der Information sowie der Einbindung von Beschäftigten bildet die umfassende Einwilligung, die dem gesamten Datenumgang eine sichere Rechtsgrundlage verleiht. Im Kontext der digitalen BGF müssen bei der Einwilligung besondere Herausforderungen berücksichtigt werden, schließlich handelt es sich um sensible Daten zum mehr oder weniger guten Gesundheitszustand, die in einem Umfeld erfasst werden, in dem Leistung beziehungsweise Leistungsfähigkeit eine ganz entscheidende Rolle spielen. Hinzu kommt, dass es insbesondere bei digitalen Lösungen eine Vielzahl an beteiligten Parteien gibt (unter anderem Arbeitnehmer, Arbeitgeber, BGF-Dienstleister, Smartphone-Hersteller, Telekommunikationsanbieter, App-Programmierer), was die Frage aufwirft, wer hinsichtlich des Datenumgangs über welche Rechte und Möglichkeiten verfügt. In Bezug auf die Gestaltung einer Einwilligung sind zunächst fünf allgemeine Anforderungen zu erfüllen (zur näheren Definition dieser Begriffe siehe Kasten rechts):

- Freiwilligkeit
- Bestimmtheit
- Angemessenheit
- Widerruflichkeit
- Informiertheit

Insbesondere an die Frage, ob der Einwilligende tatsächlich ausreichend informiert wurde, werden hohe Anforderungen gestellt. Im Einzelnen sollten bei der Information die folgenden Aspekte genau spezifiziert werden:

Zweck der BGF-Maßnahme: Die bloße Information, dass es sich um eine gesundheitsfördernde Maßnahme handelt, ist nicht hinreichend. Stattdessen sollte detailliert ausgeführt werden, welche Absicht hinter den einzelnen Maßnahmen steht. Wird etwa ein Aktivitäts-Tracker eingesetzt, so sollten die Betroffenen informiert werden, ob dies lediglich zum Zwecke einer individualisierten Rückmeldung erfolgt, ob diese Informationen in einen Bericht für das Unternehmen einfließen oder ob beispielsweise die Gesamtschrittzahl aller Beschäftigten am Unternehmensstandort A mit jener vom Standort B verglichen wird.

Art der Daten und Umgang damit: Es sollte dargestellt werden, welche Daten auf welche Art und Weise erhoben und wie diese nachfolgend verarbeitet werden. Dazu zählt die Information, um welche Datenkategorien (zum Beispiel Fragen zum Aktivitätsverhalten) oder welche Datenfelder (zum Beispiel Messung mittels Schrittzähler) es sich handelt. Ebenso sollte ausgeführt werden, ob die Daten von Betroffenen selbst geliefert (zum Beispiel durch Beantwortung von Fragen auf dem Smartphone), automatisch erfasst (zum Beispiel zu Fuß zurückgelegte Strecke mittels GPS) oder womöglich von Dritten eingegeben werden (zum Beispiel

ÜBERBLICK

Chancen digitaler BGF	Risiken digitaler BGF
Erschließung neuer, bisher vernachlässigter Zielgruppen • Außendienstmitarbeiter • Beschäftigte an kleinen Standorten • Beschäftigte auf Reisen oder im Homeoffice • junge, technologieaffine Beschäftigte	Datensicherheit und Datenschutz • Unklarheit bezüglich des Speicherorts der Daten und des Zugriffs darauf • Art und Umfang der erfassten Daten • Dauer der Datenspeicherung • Datennutzung und Datenmissbrauch durch den Arbeitgeber oder Dritte
Vernetzung von individueller und unternehmerischer Gesundheitsförderung	Überforderung der Nutzer mit Technik und im Umgang mit eigenen Gesundheitsdaten
Elemente mit Gamification-Ansatz ermöglichen Abteilungswettbewerbe oder Standortvergleiche	Weitere Zunahme des ohnehin hohen Medienkonsums
Mögliche Nutzung als Controlling-Instrument	Fragwürdige Qualität und Messgenauigkeit vieler Angebote
Steigerung der Arbeitgeberattraktivität	

Während die Befürworter der digitalen BGF in erster Linie die vielfältigen Potenziale dieser Entwicklung ins Feld führen, bringen die Kritiker vor allem Bedenken hinsichtlich der Datensicherheit und des Datenschutzes zum Ausdruck.

CHECKLISTE

Anforderungen an die Einwilligung

Um rechtlich wirksam zu sein, muss eine Einwilligung die folgenden fünf Voraussetzungen erfüllen. Besonderes Augenmerk sollte dabei auf die ausreichende Informiertheit des Zustimmenden gelegt werden.

☐ **Freiwilligkeit**	Eine (Weiter-)Beschäftigung des Beschäftigten darf nicht an die Teilnahme an BGF-Maßnahmen mitsamt der Erhebung und Nutzung personenbezogener Daten gekoppelt sein.
☐ **Bestimmtheit**	Die Einwilligung erfolgt stets für einen bestimmten und vorab definierten Zweck und stellt somit keine Generalermächtigung dar.
☐ **Angemessenheit**	Vorformulierte Einwilligungstexte dürfen die betroffenen Mitarbeiter nicht unangemessen benachteiligen. Sie unterliegen derselben Angemessenheitskontrolle wie Allgemeine Geschäftsbedingungen (AGB).
☐ **Widerruflichkeit**	Die abgegebene Einwilligung kann im Verlauf der BGF-Maßnahmen widerrufen werden, ohne dass Konsequenzen zu befürchten sind (siehe Freiwilligkeit).
☐ **Informiertheit**	Der Einwilligung muss eine detaillierte Aufklärung vorausgehen („informed consent").

FAZIT UND HANDLUNGSEMPFEHLUNGEN

- BGF und Datenschutz lassen sich in Einklang bringen
- Datenumgang technisch und organisatorisch sicher ausgestalten
- betrieblichen Datenschutzbeauftragten sowie gegebenenfalls Betriebsrat frühzeitig einbeziehen
- Datenumgang für Beschäftigte transparent machen
- Einwilligung der betroffenen Mitarbeiter einholen
- Anforderungen an eine Einwilligung beachten, unter anderem deren Freiwilligkeit

Blutdruckwerte vom Betriebsarzt). Bezüglich der weiteren Verarbeitung sollten die Beschäftigten zudem informiert werden, an welchem Ort Daten verarbeitet werden. Es sollte Klarheit bestehen, ob Daten nur auf dem Client des Beschäftigten (PC, Tablet, Smartphone oder anderes Device) gespeichert werden, auf dem sie nach Ende der Maßnahme eigenständig gelöscht werden können, oder auf einem Server beispielsweise des Arbeitgebers, des BGF-Dienstleisters oder eines Rechenzentrums.

Datenzugriff: Ergänzend sollten die Befragten dahingehend aufgeklärt werden, wer Zugriff auf die eingegebenen beziehungsweise automatisch ermittelten Daten hat. Zugriffsrechte können sich beispielsweise auf den Mitarbeiter selbst beschränken oder aber für technische Administratoren bestehen (zum Beispiel BGF-Dienstleister, Rechenzentren, auch extern eingebundene Dienstleister) und medizinisches Fachpersonal (zum Beispiel Betriebsarzt).

Darüber hinaus sollte aus der Aufklärung hervorgehen, welche Ergebnisse den verschiedenen Parteien abschließend zugänglich gemacht werden sollen und dürfen – insbesondere, welche Form der Rückmeldung die Beschäftigten erhalten (zum Beispiel individueller Gesundheitsbericht) und welche der Arbeitgeber (zum Beispiel Projektbericht mit aggregierten und anonymisierten Ergebnissen).

Ebenso müssen die Hauptverantwortlichen genannt sein, an die sich die Beschäftigten wenden können, wenn sie Fragen zur Datenverarbeitung haben, die Korrektur bereits getätigter Angaben wünschen oder ihre Einwilligung zurückziehen möchten.

Papier oder digital: Formale Aspekte bei der Einwilligung

Bei der formalen Ausgestaltung der Einwilligung kann zwischen Papierform und elektronischer Variante unterschieden werden. Wird die Einwilligung in Papierform eingeholt, so müssen ihr die oben genannten Informationen beiliegen. Zudem ist eine handschriftliche Unterzeichnung nötig. Bei einer Einwilligung in elektronischer Form ist zu beachten, dass eine eindeutige und bewusste Erklärung zu erfolgen hat. Dies kann mittels einer Check-Box realisiert werden, bei der die betroffene Person an der entsprechenden Stelle ein Häkchen setzt. Dieser Vorgang muss vom verantwortlichen Anbieter protokolliert werden. Technisch muss gewährleistet sein, dass während des Einwilligungsvorgangs die oben genannten Informationen einsehbar sind und auch später jederzeit abgerufen werden können. Dazu hat sich in der Praxis ein zweistufiges Verfahren bewährt: Zusammen mit der Einwilligung im engeren Sinne, die zwingend zu passieren ist, indem ein Häkchen gesetzt wird, findet sich auf der gleichen Seite ein eindeutig beschriebener Link, der auf eine separate Seite mit weiteren Detailinformationen zum Datenumgang und Datenschutz führt. ■

DR. FABIAN KRAPF ist wissenschaftlicher MItarbeiter am Institut für Betriebliche Gesundheitsberatung (IFBG).

DR. UWE KLAUS SCHNEIDER ist Rechtsanwalt, Fachanwalt für IT-Recht und Sozius der Kanzlei Vogel & Partner.

DR. UTZ NIKLAS WALTER ist wissenschaftlicher Leiter des Instituts für Betriebliche Gesundheitsberatung (IFBG).