WilhelmGilliéron
AVOCATS

Auteur: Wilhelm Gilliéron Avocats | Le : 4 Oktober 2021

Datenschutz und freie Berufe: gar nicht so kompliziert

Am 10. Juni 2021 verhängte die italienische Datenschutzbehörde gegen einen Zahnarzt eine Geldstrafe in Höhe von 20 000 Euro mit der Begründung, der Zahnarzt habe sich geweigert, einen HIV-Patienten zu behandeln, ohne deutlich darauf hinzuweisen, dass eine solche Offenlegung zu einer Verweigerung der Behandlung und nicht nur zu Konsequenzen für die mögliche Behandlung führen könnte.

Auch wenn es sich hier um einen Sonderfall handelt, so wird doch mit der Annahme aufgeräumt, dass die Einhaltung des Datenschutzes nur große Unternehmen betrifft, die als einzige in der Lage sind, personenbezogene Daten in großem Umfang zu verwerten, und die daher als einzige ins Fadenkreuz der Behörden und möglicher Sanktionen geraten.

Es stellt sich die Frage, welche Maßnahmen Ärzte, Zahnärzte und andere Juristen (die ich der Einfachheit halber im Folgenden als „Praktiker“ bezeichne) vernünftigerweise ergreifen sollten, um ein Missgeschick zu vermeiden.

A. ***Keine Anwendung der RGPD***

In Wirklichkeit sind diese Schritte recht einfach. Zunächst ist daran zu erinnern, dass die Praktiker, sofern sie sich an in Europa ansässige Personen nicht wenden, nicht der RGPD, sondern nur dem Bundesgesetz über den Datenschutz unterliegen, dessen Revision im Laufe des Jahres 2022 in Kraft treten dürfte.

2. ***Rechtliche Verpflichtungen***

Ohne ins Detail zu gehen, gibt es drei Hauptpflichten für Praktiker, von denen die ersten beiden im Auge behalten werden sollten:

1. **Das Register der Verarbeitungstätigkeiten**

Die Verpflichtung zur Führung eines Tätigkeitsregisters erfordert grundsätzlich, dass unter anderem die Art der Verarbeitung, der Zweck der Verarbeitung, die Kategorien von Personen (Patienten, Beschäftigte, manchmal Lieferanten) und die Kategorien personenbezogener Daten (die im medizinischen Bereich sensibel sein können), die verarbeitet werden, sowie mögliche Übermittlungen ins Ausland und die Empfänger dieser möglichen Übermittlungen festgelegt werden.

Der Bundesrat hat jedoch Unternehmen mit weniger als 250 Beschäftigten von dieser Verpflichtung ausgenommen, wenn die betreffende Verarbeitung nicht in großem Umfang mit der Verarbeitung sensibler Daten verbunden ist oder nicht zur Erstellung eines Hochrisikoprofils führt. Auch wenn ein risikoreiches Profiling für Praktiker von vornherein ausgeschlossen werden kann, ist die Verarbeitung sensibler Daten, insbesondere im medizinischen Bereich, durchaus möglich. Das Erfordernis des „großen Umfangs“ scheint jedoch eine massive Verarbeitung innerhalb eines Krankenhauses oder einer Klinik vorauszusetzen, was bei einer Privatpraxis auf den ersten Blick nicht der Fall sein dürfte.

Dies ist eine Verpflichtung, von der die Praktiker befreit werden sollten.

2. **Die Informationspflicht**

Alle für die Datenverarbeitung Verantwortlichen, einschließlich praktizierender Ärzte, sind grundsätzlich verpflichtet, die betroffene Person angemessen über die Erhebung personenbezogener Daten und den Zweck der Erhebung zu informieren (d. h. wofür die Daten verwendet werden sollen und warum ihre Erhebung notwendig ist).

Eine solche Verpflichtung ist zwar leicht umzusetzen, doch sieht das Gesetz vor, dass der für die Verarbeitung Verantwortliche von dieser Verpflichtung befreit ist, wenn es sich um eine Privatperson handelt, die einer gesetzlichen Geheimhaltungspflicht unterliegt. Die Ärzte unterliegen einer solchen Verpflichtung gemäß Artikel 321 des Strafgesetzbuches; es ist daher davon auszugehen, dass sie rechtlich nicht verpflichtet sind, ihre Patienten oder Kunden über die durchgeführten Behandlungen zu informieren.

Es gibt jedoch eine Ausnahme von diesem Grundsatz. Erfordert die vorgesehene Verarbeitung die Verarbeitung sensibler Daten, wie z. B. medizinischer Daten, so ist die ausdrückliche Einwilligung der betroffenen Person erforderlich, was bedeutet, dass diese ordnungsgemäß über die betreffende Verarbeitung informiert werden muss, damit ihre Einwilligung gültig ist, wobei im schweizerischen Recht, anders als im europäischen Recht, die Einwilligung auch dann als ausdrücklich gilt, wenn sie unter Bezugnahme auf allgemeine Bedingungen erteilt wird.

3. **Angemessene Sicherheitsmaßnahmen**

Letzten Endes sind es die Pflichten der Praktiker, die dafür sorgen müssen, dass angemessene Sicherheitsmaßnahmen zum Schutz der Daten vor den damit verbundenen Risiken getroffen werden, die am wichtigsten sind.

Welche Ratschläge können den Praktikern daraus gegeben werden?

3. ***Praktische Überlegungen***

1. **Zur technischen Seite**

Drei Bemerkungen:

- Erstens muss der Praktiker dafür sorgen, dass seine Infrastruktur eine gewisse Sicherheit für die Daten seiner Patienten oder Kunden gewährleistet. In diesem Zusammenhang ist anzumerken, dass die Inanspruchnahme eines **Cloud-Anbieters** inzwischen weithin akzeptiert wird, sofern dieser als Hilfskraft (in gleicher Weise wie Verwaltungspersonal) des Arztes erscheint; die Beauftragung eines solchen Anbieters mit der Verarbeitung von Daten scheint daher keinen Verstoß gegen Artikel 321 des Strafgesetzbuchs darzustellen. Idealerweise sollten sich die Server des Anbieters in der Schweiz oder zumindest in Europa befinden (ein Standpunkt, der hier hinsichtlich der Zulässigkeit eines Anbieters außerhalb der Schweiz, aber in Europa, umstritten ist), und sie sollten bestimmten Zertifizierungen als Sicherheitsgarantie unterliegen, wie z.B. der Norm ISO27001. Es spricht jedoch nichts dagegen, einen **internen Server zu** haben, der **ordnungsgemäß** durch eine Firewall oder ein VPN **geschützt ist**, wenn die Berufsausübung, insbesondere bei Anwälten und Telearbeitern, Fernarbeit beinhaltet.

- Zweitens sollte eine **Zugangskontrolle eingerichtet werden**, da es oft nicht gerechtfertigt ist, dass das gesamte Verwaltungspersonal Zugang zu allen potenziell sensiblen Daten der behandelten Patienten hat oder dass jeder Mitarbeiter weiß, wie viel seine Kollegen verdienen. Hier sollte der angelsächsische Grundsatz der „*need to know basis*“ gelten.

- Schließlich sollte man es vermeiden, unprofessionelle E-Mail-Adressen zu verwenden, wie es leider einige im medizinischen Bereich tun, wie z. B. hotmail, Gmail oder bluewin. Außerdem sollte die Verwendung eines Instant-Messaging-Systems wie What’s App in der Berufswelt vermieden werden, es sei denn, der Patient oder Klient bittet ausdrücklich darum und stimmt zu (und besteht darauf, möchte ich hinzufügen). Empfehlenswert ist die Verschlüsselung von E-Mails, die inzwischen einfach ist (siehe Anbieter wie www.swisssign.com).

2. **Auf der Informationsseite**

Auch wenn wir gesehen haben, dass sich die Informationspflicht eigentlich auf die Verarbeitung sensibler Daten (z. B. medizinischer Daten) beschränkt, für die eine ausdrückliche Zustimmung erforderlich ist, ist es dennoch einfach und meines Erachtens eine gute Praxis, hier ein gewisses Maß an Transparenz zu fördern, was mit weniger Aufwand auf zwei Arten geschehen kann:

- Erstens durch die Verabschiedung einer **Datenschutzerklärung, die** auf der Website oder in Form eines Flyers im Wartezimmer ausgehängt wird und in der Regel folgende Punkte enthält (1) welche Daten werden verarbeitet; (2) zu welchen Zwecken; (3) mit wem teilen wir Ihre Daten? (4) wo werden sie verarbeitet, (5) wie lange werden sie gespeichert und (6) welche Rechte haben Sie? Dies war die Entscheidung von Wilhelm Gilliéron Anwälte AG, die es als Spezialist für Datenschutz schwierig fand, keine Politik zu diesem Thema zu haben, die Sie hier finden können.

- Zweitens, und insbesondere im medizinischen Bereich, wo es üblich ist, vor jeder Konsultation ein **Formular auszufüllen**, ist die Verwendung eines solchen Formulars eine praktische und einfache Möglichkeit, darin den Zweck der Erhebung bestimmter Daten (insbesondere Gesundheitsdaten, für die eine ausdrückliche Zustimmung erforderlich ist), die Art und Weise, wie sie aufbewahrt werden, wie lange sie aufbewahrt werden und an wen sie weitergegeben werden, zu erwähnen.

3. **Verschiedene**

Schließlich kann nicht oft genug betont werden, dass eine Datenübermittlung ins Ausland nur mit der ausdrücklichen Zustimmung der betroffenen Person erfolgen sollte und dass die verarbeiteten Daten nach einem festzulegenden Zeitraum (in der Regel gesetzlich festgelegt) gelöscht werden müssen, sobald die betroffene Person nicht mehr Patient oder Kunde ist (z. B. 20 Jahre bei Zahnärzten).

4. ***Schlussfolgerung***

Auch wenn das Bundesdatenschutzgesetz und der große Medienrummel, den es auslöst, beängstigend sein mögen, so ist es für freiberuflich Tätige doch einfach, ihm mit einer Reihe von Maßnahmen zu entsprechen, die alles in allem minimal sind: eine angemessene Datenschutzerklärung, ein Formular, das es ermöglicht, die ausdrückliche Zustimmung im Falle der Verarbeitung sensibler Daten sicherzustellen (auch wenn eine Unterschrift an sich nicht unbedingt erforderlich ist) und vor allem angemessene Sicherheitsmaßnahmen, die nur das Ergreifen von Maßnahmen erfordern, die alles in allem recht einfach sind.

Source : https://www.wg-avocats.ch/de/nachrichten/datenschutz/datenschutz-freie-berufe/